Design and Performance Aspects of Information Security Prediction Markets for Risk Management

Pankaj Pandey and Einar Arthur Snekkenes
Norwegian Information Security Lab., Gjovik University College, Teknologivn. 22, 2815 Gjovik, Norway

Keywords: Information Security, Security Economics, Security Risk Management, Prediction Market.

Abstract: Prediction Markets are the markets designed and operated to mine and aggregate the information scattered among the traders. Recently, some researchers have started exploring the application of prediction markets in the information security domain. The information security prediction market will facilitate trading of contracts to hedge the financial impact of the risks associated with the underlying information security events, such as discovery of a vulnerability in a piece of software. However, prediction markets differ in their objectives and requirements, and therefore information security prediction markets need to be carefully engineered to meet the specific requirements. The contribution of this paper is the identification of a set of design requirements for an information security prediction market, and associated performance criteria. We present five categories of design requirements: Contracts, Trading Process, Participants and Incentives, Clearing House, and Market Management for the information security prediction market. Furthermore, we present six performance measures: Information Elicitation, Transparency, Efficiency, Transaction Cost, Liquidity, and Manipulation Resistance for the performance assessment of information security prediction market.

1 INTRODUCTION

The Global Risk report of World Economic Forum states that "Effective methods for measuring and pricing cyber risks may even lead to *new market-based risk management structures* which would help in understanding the systemic interdependencies in the multiple domain that now depend on cyberspace" (WEF, 2014). A carefully designed Prediction Market can be used as a market mechanism for the management of information security risks.

Prediction markets are the markets designed and operated for mining and aggregation of information which is scattered among the market participants (Berg and Rietz, 2003). Subsequently this information is reflected in the market prices and the prices have a strong correlation with the probability belief of the traders (Luckner, 2008). Prediction markets have been used for various purposes such as prediction of government policy actions, weather events, economic indicators, elections, etc. (Luckner, 2008). Prediction markets have also been attempted in the security and terrorism domain. A well known (now abandoned) project in the security domain is "Future Markets Applied to Prediction (FutureMAP)" project of Defense Advanced Research Project Agency (DARPA), USA (Hanson, 2006). FutureMAP was to be used as an "Electronic Market-Based Decision Support" system to improve the approaches for collection of intelligence information (Hanson, 2006).

(Pandey and Snekkenes, 2014a) assessed the applicability of prediction markets in the information security domain as a risk management tool in an intra-organizational setting as well as in an open setting. The usefulness of prediction markets in hedging the (financial impact of)information security risks is explained in (Pandey and Snekkenes, 2014b). As the prediction markets differ in their objectives and requirements, an important question in the context of information security prediction markets (ISPM) is: how to design and engineer an ISPM to achieve the objectives of information aggregation and risk management? The primary contribution of this article is the identification of a set of design elements and associated performance measures for ISPM.

The remainder of the paper is structured as: Section 2 explains the research method followed for the article. Section 3 presents the related work. Section 4 presents the design requirements for an ISPM. Section 5 explains the design elements of an ISPM. Section 6 presents the performance measures for an ISPM. Section 7 resents the conclusion and directions for future work.

Pandey P. and Arthur Snekkenes E..
Design and Performance Aspects of Information Security Prediction Markets for Risk Management.
DOI: 10.5220/0005547502730284
In *Proceedings of the 12th International Conference on Security and Cryptography* (SECRYPT-2015), pages 273-284
ISBN: 978-989-758-117-5

2 RESEARCH METHOD

The research follows the Design Science Research Approach (DSRA). DSRA is useful when innovations and ideas are created for development of technical capabilities and products which will be instrumental in effective and efficient process development for artefacts (Johannesson and Perjons, 2014). The steps in DSRA are as follows:

1. *Explicate Problem :* The first step is to formulate the initial problem, justify its importance and investigate the underlying causes (Johannesson and Perjons, 2014). To explicate the problem we started with examining the literature on information security markets, and taxonomy of prediction markets to design an ISPM. This enabled us in identifying the limitations of existing market engineering frameworks. An overview of reviewed literature is covered in Section 3.
2. *Define Requirements :* The second step is to identify and outline an artefact to address the explicated problem and to elicit requirements for the artefact (Johannesson and Perjons, 2014). A requirement is the property of the artefact that is desired by stakeholders in practice and is used for design and development of the artefact. A requirement can be functional, structural, or environmental in nature. The requirements for the artefact (ISPM) are given in Section 4.
3. *Design, Development and Demonstration of the Artefact :* The next step leads to creation and demonstration of an artefact that fulfils the requirements identified in the previous (second) step. This includes designing the functionality and structure of the artefact (Johannesson and Perjons, 2014). The demonstration shows that the artefact can, in fact, solve the problem (or some aspects of it) in the given situation. The functionality and structure of the artefact (ISPM) are demonstrated in Section 5.
4. *Evaluation of the Artefact :* The last step is to evaluate the artefact. This determines the extent to which the artefact is able to solve the explicated problem and its requirements (Johannesson and Perjons, 2014). We have not evaluated the artefact (ISPM) in the strictest sense; however we have identified the performance factors for ISPM in Section 6. We have used the 'informed argument' form of evaluation. In this form, researchers evaluate the artefact by reasoning and arguments for its usefulness in meeting the defined requirements and solving the explicated problem. Informed argument form of evaluation is often used to evaluate the artefacts which are highly innovative and are still immature.

3 RELATED WORK

(Weinhardt and Gimpel, 2007) defined a market as "a set of humanly devised rules that structure the interaction and exchange of information by self-interested participants in order to carry out exchange transactions at a relatively low cost". The efficiency and effectiveness of the market in achieving the specific objectives depends upon the design and implementation of the market.

(Spann, 2002) proposed a taxonomy for the implementation of (prediction) markets. This taxonomy has five elements with several sub-components, namely Market Strategy, Market Design, Information Design, Market Operations and Data Interpretation. Out of the five elements only one element, i.e. Market Design is relevant for this article. The 'Market Design' comprises of six elements: Underlying (event), Medium of Exchange, Incentive System, Trading Mechanism, Market Rules and Kick Off Settings.

(Weinhardt and Gimpel, 2007) proposed a 'Market Engineering Framework' to define a structured, systematic and theoretically grounded process of design, implementation, evaluation and introduction of market platforms. (Plott and Chen, 2002; Luckner, 2008; Sripawatakul and Sutivong, 2010) also present some guidelines on the design and implementation of prediction markets.

However, due to various legal, intellectual property and security reasons (Fidler, 2014), the design and implementation issues discussed in the above articles do not suffice to address the specific requirements and objectives of the ISPM. Further, we need specific parameters to understand and assess the performance of an ISPM.

4 REQUIREMENTS FOR ISPM

From our systematic review of literature on design and implementation of prediction markets (Luckner, 2008; Weinhardt and Gimpel, 2007; Spann, 2002; Plott and Chen, 2002; Sripawatakul and Sutivong, 2010), and existing market methods for management of information security risks (Fidler, 2014) we have identified 13 key design requirements for an ISPM. As shown in Table 1, the design requirements are grouped into five categories: (i) Contracts, (ii) Trading Process, (iii) Participants and Incentives, (iv) Clearing House, and (v) Market Management.

Table 1: Requirements for ISPM.

Contracts	Type of Contracts Contract Specifications
Trading Process	Trading Mechanism Anonymous Trading
Participants and Incentives	Participant's Motivation Incentive Structure
Clearing House	Contract Settlement Criteria Counterparty Risk Management Trusted Third Party Intellectual Property Management Know Your Trader
Market Management	Regulated Market Legal Permission

5 DESIGN ASPECTS OF ISPM

This section explains the design requirements identified in section 4. This section is divided into five subsections, each for one group of design requirements. The five subsections are further divided into thirteen sub-subsections each for one design aspect of ISPM.

5.1 Contracts

An ISPM will be a marketplace to buy and sell contracts with underlying security events. The contracts must be specific and all the details regarding the decision criteria, payoff, settlement date, etc. should be specified before the contract is made available for trading. The contract price will be an approximate measure of the probability, mean or median of the underlying events at any time. The ability to use market prices as forward-looking indicators of security properties will help in establishing information symmetry between buyers and sellers (i.e. build a quality signal), and help security stakeholders to make better and more informed decisions, by differentiating mediocre security products from good ones. The contract types and specifications are explained below.

5.1.1 Contract Types

On the basis of payoff mechanism, the contracts can broadly be categorized into three types: (i) Binary contracts, (ii) Index contracts, and (iii) Spread contracts. A comparison of contract types is shown in Table 2.

- *Binary Contracts:* In binary contracts the payoff is linked to the occurrence or non-occurrence of the underlying event. For example, A binary contract that pays $100 to the buyer of the contract depending on whether the biometric system of smartphone 'XYZ' will be found vulnerable to a spoofing attack by the 31/Mar/2015.If somebody thinks that the vulnerability does not exist or will not be found by the contract expiry date, then the individual will sell the contract. The price of contract will be in the range of $1 to $100, depending on the beliefs of market participants. For binary contracts, with a settlement value of $100, the actual settlement value will be $0 or $100.

Table 2: Comparison of Contract Types.

Contract Type	Payoff Mechanism	Market Belief
Binary	All or Nothing	Probability
Index	Proportionate to outcome	Mean
Spread	Double if outcome exceeds cutoff else nothing	Median

- *Index Contracts:* In case of index contract, the value of the contract is linked to the outcome of the underlying event. For example, an index contract that pays $0.01 for every data breach disclosed between 01/Mar/2015 to 31/Mar/2015, and if A thinks that 40 or more such incidents will be disclosed and B thinks that 80 or less such incidents will be reported, then the market price will be between $0.39 and $0.81. A will buy for strictly less than $0.40 (i.e. $0.39), and B will sell for strictly more than $0.80 (i.e. $0.81).
- *Spread Contracts:* Spread contracts can be used to bet on whether the outcome related to the underlying event will be above or below a certain value, i.e. the spread. In spread contracts, the current market price can be interpreted as the traders' expectation of the median outcome of the underlying event. Let us consider a contract with the underlying event being the discovery of a vulnerability in a software. Let us say the market maker is quoting at the price (spread) $50-$55, i.e. the market maker wants to buy at $50 and sell at $55. If a trader believes that the price will go up (i.e. a vulnerability will be discovered) he will buy from the market maker at $55. If after some time, some new relevant information is known to the market participants and the current quote by market maker is $60-$65. Then, if the trader who purchased the contract at $55 wants to cash out his profits, he will sell his contracts at $60 to the market maker.

5.1.2 Contract Specifications

An important aspect of contract design is the precise specification of the contract. The contract specifications should clearly mention the expiry date, settlement date (settlement date can be different from the expiry date), payoff, decision criteria and other factors relevant to the underlying event.

For instance, for a contract which is meant to allow betting on discovery of vulnerability 'V' in the software 'S' on or before the date 'D', the contract specifications must clearly define the vulnerability 'V' as in what is included and what is not. Secondly, the specification should include information on the source which will be considered for the acceptance or rejection of the vulnerability. The source can be a government body regularly reporting such information, appearance of the said information in the regular media, reporting by responsible organization such as Google through its 'ProjectZero' (Google, 2014), or a direct reporting by the vulnerability discoverer to the market operator.

If the vulnerability can be directly reported to the market operator then the contract should clearly specify the testing procedure or the testing body which will certify the existence of the vulnerability. Further, a proper policy should be crafted regarding the responsible reporting of vulnerability to the vendor and the time period during which the vulnerability information will be kept secret. In such a scenario when the vulnerability 'V' is directly reported to the market operator and it is reported on or before the date 'D' but it needs to be kept secret for sometime, then the contract will expire on the date mentioned as expiry date specified on the contract but the settlement of the contract will take place only after the vulnerability has been tested and reported to the vendor. It is not necessary to wait for the vulnerability patch. The market operator may set a fix period within which the vendor is expected to release the patch. However, if the vendor fails to fix the vulnerability within the given period, the contract will be settled and vulnerability information (full or partial) will be made public.

As the information security events and therefore the information security contracts are different from the traditional sports or political contracts, it is important to clearly define the underlying event and the decision criteria, otherwise an ambiguity in specifications may lead to disputes and confusion. The concern for ambiguity and confusion is likely to be anticipated by the buyers and sellers. Thus in addition to 'noise' during the clearing process, buy/sell prices will be affected by the concern. The cost of trust (of outcome decision) will be factored into prices offered by the buyer and seller, thus with low trust, there might not be any trade.

A closely related real world example is from TradeSports (TradeSports, 2015). In 2006 TradeSports had a contract with a payoff value of 100 if North Korea would launch a test missile and the missile leaves North Korean air space on or before 11:59:59pm ET on 31st July 2006 otherwise the will pay 0 (EOG, 2006). The source to be used for the settlement of the contract was the U.S. Department of Defense. In early July 2006, the Government of North Korean claimed to have conducted such a test and this was reported by various news sources as well. However, the U.S. Department of Defense did not confirm the test leading to the settlement of the contract at 0. Had the contract mentioned some other source for the decision the contract could have settled at 100. On the other hand if the contract had multiple sources of confirmation then this could have led to disputes between the traders and the operator.

5.2 Trading Process

Trading process is divided into two parts, namely trading mechanism and anonymous trading, and are explained below.

5.2.1 Trading Mechanisms

The selection of trading mechanism depends upon the type of contract and its specification. As the information security prediction markets are meant to provide a risk management mechanism, it is extremely important that the market participants are allowed to adjust their bets based on the latest information they may have about the underlying event.

(Pennock, 2004) identified four types of trading mechanisms, (i) Continuous Double Auction; (ii) Continuous Double Auction with Market Maker; (iii) Pari-mutual Market; and (iv) Market Scoring Rule. However, Pari-mutual market mechanism does not allow continuous incorporation of information and therefore it is not useful for the information security prediction market. (Pennock, 2004) proposed a new trading mechanism called Dynamic Pari-mutual Market, and this mechanism provides the continuous incorporation of information. These trading mechanisms are compared on the basis of four criteria: (i) Continuous incorporation of information; (ii) Liquidity guarantee; (iii) Ability to cash out anytime during the market trading hours; and (iv) Bounded risk to market operator.

- *Continuous Double Auction (CDA):* CDA is a widely used mechanism in the financial markets. In this model, limit order book is used to match

buy orders with the sell orders. The orders are matched based on the price and time priority. Apart from the limit orders, any trader can buy at the best ask price and sell at the best bid price.

- *Continuous Double Auction with Market Maker (CDAwMM):* CDAwMM is a bookie mechanism which is used in sports betting. This mechanism is like CDA with an automated market maker which guarantees market liquidity by transferring the risk to the market operator. The mechanism allows continuous incorporation of information.
- *Dynamic Pari-Mutuel Market (DPM):* DPM was proposed by (Pennock, 2004). In DPM mechanism, traders are allowed to purchase shares at any time and on any outcome. This mechanism provides an automated market maker which provides infinite liquidity to the buyers. The trading prices are set by the market maker on the basis of a predetermined pricing formula. The pricing of contracts allows continuous incorporation of information. However, the market maker does not buys the shares from traders and the CDA mechanism is used to allow selling of contracts by traders.
- *Market Scoring Rule (MSR):* MSR was proposed by (Hanson, 2003) for trading in prediction markets . He suggested that a scoring rule can be used to allow betting on the entire probability distribution over many variables and a scoring rule will reward the traders for incremental improvements in the outcome. All the traders are allowed to see the current probability distribution and if a trader thinks that the current probability is incorrect then the trader can readjust the probability. In this case, each new predictor is paid off for improving the prediction probability and traders lose money if their prediction is worse. The final pay off depends on the closeness of trader's predictions to the actual outcome.

Table 3 presents a comparison of trading mechanisms.

Table 3: Comparison of Trading Mechanisms.

	CDA	CDA wMM	DPM	MSR
Continuous Information Incorporation	Yes	Yes	Yes	Yes
Liquidity Guarantee	No	Yes	Yes	Yes
Anytime Cash Out in Market Hours	Yes	Yes	Yes	Yes
Bounded Risk to Market Operator	Yes	No	Yes	Yes

5.2.2 Anonymous Trading

Anonymous trading implies that the identification information about traders is not revealed to market participants. In anonymous trading system, traders with private information are more likely to participate, as it would be extremely difficult for other traders to distinguish between the orders and trades coming from an informed and an uninformed trader. Furthermore, threats of retribution by the employer of the trader can deter the trader participation. On the other hand, security researchers working in the field may face certain ethical concerns or peer pressure against the participation in the market. In such cases, anonymous trading will let the insiders with private information to trade in the market. This will improve the information aggregation and the overall performance (efficiency) of the market.

5.3 Participants and Incentives

Market participants and participation incentives are two key design aspects of information security prediction markets. These two factors are explained below.

5.3.1 Participant's Motivations

ISPMs are expected to attract at least six types of participants: (i) Product Users; (ii) Cyber-Insurance Providers; (iii) Investors; (iv) Product Vendors; (v) Product Vendor Competitors; (vi) Security Researchers. Each of these users may have unique or similar motivations to participate in the market. For instance for a contract such as : Vulnerability 'V' will be discovered in Product 'P' on or before 11:59:59 PM(GMT) 31/Mar/2015. The motivation for each of the participant type to trade in the above contract is shown in Table 4.

5.3.2 Incentive Structure

An appropriate incentive structure is required to motivate traders to participate in the market and truthfully reveal the information relevant to the underlying the event. The incentives for participation in a prediction market are either monetary incentives or non-monetary incentives. However, as the goal of the ISPM is to provide a risk management mechanism for financial impact associated with the underlying information security events, the incentive structure in this case can only be monetary. The incentive structure will vary based on the payoff mechanism of contracts. Different contracts, such as binary, index, spread, bonds, insurance-linked, etc. will have differ-

ent incentive structure and some contracts may be of special interest to specific type of participants.

Table 4: Participants and Incentives.

Participants	Incentives
Product Users	To hedge the product risk
Cyber Insurance Providers	To underwrite their customer's cyber-risks
Product Vendors	To prove the security of their software, to signal its quality with respect to other vendor's products,to use it as employee stock options to incentivize developers to develop secure products
Product Vendor Competitors	To prove that the product is not as secure as their own product
Security Researchers	To earn profits from the market

5.4 Clearing House

The clearing house is a body which clears and settles all the trades in the market. In an ISPM, clearing house will play at least the following four roles.

5.4.1 Contract Settlement

Due to very technical nature of information security contracts it will not be easy and straight forward to decide on the technicalities. For example, in case of a contract associated with privacy breach at a bank, it is important to specify and define as in what constitutes the privacy breach and what is not covered in the contract specification. Thus, the clearinghouse will act as the final decision body with regards to the settlement of the contracts. Further, for the contracts related to vulnerability discovery and when the vulnerability is directly reported to the market (i.e. to the clearing house) they have the responsibility to test and accept or reject the vulnerability. This will lead to settlement of the contract and final pay outs.

5.4.2 Counterparty Risk Management

The clearing house will act as a guarantee between the two counterparties involved in the trade. This implies that the clearing house acts as a buyer for the seller of the contract and as a seller for the buyer of the contract. In case of zero net supply contracts, the clearing house has no market risk. However, it is exposed to the risk associated with failure of any of the counterparty in the market. Thus, the clearing house needs to have sufficient capital to cover the risk.

5.4.3 Trusted Third Party

The clearing house will act as a trusted third party for various activities including but not limited to verification of vulnerabilities directly reported to it, keeping the vulnerability information secret for a specified period, responsibly reporting the vulnerability to the vendor, etc.

5.4.4 Intellectual Property Management

The ISPMs are likely to have a range of contracts with various types of underlying events or information. Thus, for contracts involving some kind of intellectual property, such as development of an exploit against the specified discovery will need to be dealt in an ethical and legal way.

5.4.5 Know Your Trader

Due to the security concerns associated with the information related to the underlying events and financial aspect of trading (incentives), it is utmost important for the market (clearing house or a separate entity) to verify the credentials of the market participants. This is like the know-your-customer policy followed in the banking and financial industry.

Currently, it is extremely difficult to track down the origin of specific exploit trading in a black market. Black-hat hackers operate covertly to succeed in the game of attack and defense. This intense secrecy makes it difficult to track and prosecute the exploiter. So, to prevent the leakage of vulnerability and/or exploit information from the ISPM to a black-market, it is must to have a participant's verification policy.

Know-Your-Trader policy will also help in preventing insider trading. In the financial services sector, insider trading is defined as the trading of stocks and other securities of a publicly listed company by individuals with access to non-public information about the company. In the information security domain, an insider trading can take at least two forms: (i) A developer working for a company deliberately leaves some vulnerability in the code, so that it can be later sold in the ISPM, (ii) A software tester while working for his/her employer may find some bugs in an application, however instead of reporting it internally the individual may decide to sell the information in the ISPM.

Thus, the traders participating in information security prediction markets will have to provide some

(under the prevailing laws and regulations) information about their finances (to avoid credit default, illegal financing, etc.) and personal information. The personal information is required to fix the accountability and responsibility on the trader. If the private information held with a trader is used for some illegal activity then the trader can be investigated and held liable for the same. However, none of this information should be made available to other traders in the market.

5.5 Market Management

The two key aspects of management of information security prediction markets are regulations and legal permissions, which are explained below.

5.5.1 Regulated Market

Economic markets can broadly be classified into two forms, i.e. Free Markets and Regulated Markets. In a free market economy, the forces of supply and demand are not controlled by a government or authority. In contrast to a free market, in a regulated or controlled market, government intervenes in supply and demand through non-market methods such as laws to control the permissions to participate in the market, setting of prices, type of products or services, taxation, etc.

Markets for vulnerabilities will have several issues such as intellectual property, rights management, non-disclosure agreements, privacy issues, country specific laws, industry specific laws, etc. to be dealt in a fair manner. Thus, the information security prediction market will in most cases be regulated.

5.5.2 Legal Permissions

Currently, there are two main legal issues associated with information security prediction markets: (i) compliance with the financial market and gambling regulations; and (ii) regulations concerning the information (cyber-) security.

6 PERFORMANCE MEASURES FOR ISPM

This section presents the six performance measures required for effective and efficient functioning of ISPM, and are explained in the following subsections.

6.1 Information Elicitation

In an ISPM the price of a contract will be informative only when it is strongly correlated to actual probability of occurrence of the underlying event. We use the term 'informative price' to indicate that there is a strong - and publicly known- correlation between price and the aggregated belief of the stakeholders. Informative prices are extremely vital for the risk managers to allocate resources (deploy security controls) in an efficient and effective manner.

In financial terms there are two types of values, i.e. market and intrinsic value, associated with an information security contract. The market value of a contract is the current price at which trades can be executed. The intrinsic value is the expected present value of the contract with all the available information, and accounting for the benefits and costs associated with the contract. Since all the information is not known to all the traders and they differ in their analysis of information, they have different estimates about 'true' probability of occurrence of the underlying event. Therefore, intrinsic values are not perfect foresight indicators.

Informed traders will estimate the probability of the underlying event based on the private information as well as the information available in the public domains. If the intrinsic value estimated by informed traders is different from the current market price, then they will buy the undervalued contracts and sell the overvalued contracts. This difference between the intrinsic value and market price is due to noise. Therefore, the trading by informed traders leads to market prices closer to the intrinsic value calculated by them.

Let us assume that there are N traders trading a contract and each of them has a different estimate of occurrence of the underlying event. Let P_i be the probability estimate of the i'th trader. Further, let us say P is an unbiased estimate of T the true probability of the underlying event. In this case, the forecasted probability can be expressed as:

$$P_i = T + E_i \tag{1}$$

where E_i is the error in the probability estimate of i'th trader. As the probability estimates are unbiased, the expected forecast error is zero. However, in absolute terms the individual probability estimate errors might be quite high.

Let us assume that for each trader the desired position in the contract C_i is proportional to the difference between his probability estimate and the current market price (which indicates probability estimate of occurrence of underlying event), expressed as:

$$C_i = \mu(P_i - M) \tag{2}$$

where μ is some constant of proportionality, and M is the current market price. Thus, the i'th trader would like to buy the contract if his probability estimate is higher than the current market price. On the other hand, if the trader's estimate of probability is less than the current market price then the trader will (short) sell the contract to profit from the current higher market price (probability).

Further, let us assume that the contract is in 'zero net supply'. Derivatives like futures and options are examples of zero net supply financial products. Zero net supply means that for every winner there is a loser in the market. Thus, if we sum up the market value of all the position holders in the market, then we get an exact zero. This implies that as a whole the market is not exposed to any market risk, however this is not true for counterparties individually. Zero net supply is important because it ensures that there is no upper limit to the scale of the market.

The current market price for zero net supply contracts can be calculated by summing all the desired positions equal to the net supply and computing the resulting equation for M (Harris, 2002):

$$\sum_{i=1}^{N} C_i = \sum_{i=1}^{N} \mu(P_i - M) = \mu \sum_{i=1}^{N} P_i - N\mu M = 0 \quad (3)$$

The market price M is represented as

$$M = \frac{1}{N} \sum_{i=1}^{N} P_i \quad (4)$$

is an average of the individual probability estimates of underlying events. Substituting Equation 1 into Equation 4 gives:

$$M = T + E_{mp} \quad (5)$$

where Emp is the market price forecast error represented as follows:

$$E_{mp} = \frac{1}{N} \sum_{i=1}^{N} E_i \quad (6)$$

If the forecast errors of individual traders is independent of each other, then the law of large numbers will come into play and with an increase in the number of traders, the market price forecast error Emp will approach zero. Also, if the number of traders is small and if the individual trader errors are not identical then the average market price forecast error will be less than the average market price forecast error of individual traders. Therefore, the information security prediction markets will be most informative if the informed traders independently collect the information.

6.2 Transparency

Transparency is an important characteristics. Transparency deals with the information about the trading process such as prices, book size, etc. which is made available to the traders. The market transparency will ensure that the clearing house and market regulators are aware of the positions of individual traders. Thus, if a market participant becomes too exposed to market risk or is accumulating big positions which could affect the overall market, then the authorities can initiate the necessary risk management and legal actions.

Transparency in an ISPM can be divided into pre-trade transparency and post-trade transparency. Pre-trade transparency is about the information on bids, offers, book size, order depth and other such information which is useful before a trade has been made. Post-trade transparency is about providing information related to executed trades, such as time of trade, price at which it was executed, size of the trade, etc. The identity of traders should not be revealed to other traders, neither in pre-trade information nor in post-trade information. Further, Information related to vulnerability and/or exploits (if it has been directly reported to the market operator) cannot be fully disclosed to market participants until a patch has been released or the vendor was given adequate (as mentioned in the trading contract description) time to fix the same. However, historical trading prices, orders and other trade related and settlement information should be made available to the market participants. This information has twofold benefits. First, it lets the traders analyze the historical information and secondly the information can be used by cyber-insurance and information security rating companies for the pricing of insurance contracts and rating of product vendors respectively. Higher transparency in the market is expected to lead to transparent pricing of contracts.

Further, information security researchers currently face the problem of lack of data to validate various models of information security investments in security controls, estimating security strength of a security control, reputation of security product vendors, and so on. The data released by information security prediction markets will be highly useful in such scenarios where researchers and practitioners face the problem of lack of data. The data can further be useful in devising successful risk mitigation strategy, development of secure software, among various other benefits.

6.3 Efficiency

In an efficient market, market prices reflect all the information that can be acquired by traders and profitably acted upon (Fama, 1970). However, some information may be too expensive to acquire or of lit-

tle value if it cannot be used to profit from the trade. Therefore, market prices can never reflect all the information which informed traders can collect and act on. The market efficiency can be categorized into three types (Fama, 1970):

1. *Weak Efficient Market:* In the weak-form of efficient markets, the market prices reflect all the past information and no one can make profit by knowing the past information only. In this case, prices simply follow a random walk. Therefore, this form of market efficiency is not useful for information security prediction market.
2. *Semi-strong Efficient Market:* In the semi-strong form of efficient markets, the market prices reflect all the information available in the public domain. In this case, no one can predict the future market price by using only the information in public domain. In semi-strong form of markets, informed traders can profit by having access to some private information. In an ISPM security researchers may have private information about certain vulnerability in a software and they can profit from it. Also, if a contract is listed for discovery of a vulnerability in a particular software then security researchers can use their domain knowledge to discover the said vulnerability before the expiry date, thus making profit from trading in the market.
3. *Strong-Form Efficient Market:* In the strong form of efficient markets, the market prices reflect all the information available in the public domain as well as the private information as soon as it is known. In such a scenario, informed traders have no advantage over uninformed traders and therefore they can never make profit in the market. Therefore, this type of market efficiency is not useful for ISPMs.

6.4 Transaction Cost

Transaction cost will include all the cost associated with trading in the ISPM. These costs can be divided into following three categories (Harris, 2002):

- *Explicit Transaction Costs:* This includes costs like brokerage paid, exchange fees, taxes paid. This also includes cost of acquiring relevant information such as information related to a vulnerability, software product, etc. Further, it includes the cost associated with time spent and resources used by a security researcher to discover vulnerability in a software. The security researcher can use this private information about the existence of vulnerability in the software to trade relevant contract(s) listed on the information security prediction market.
- *Implicit Transaction Costs:* This type of trading cost arises when traders have an impact upon the market prices. For instance, if a trader buys at the ask price and sells at the bid price then he ends up paying the bid-ask spread price. Similarly, when traders push up the price while executing large buy orders, and push down the prices when executing a large sell order, the impact of their trading on the prices constitutes transaction cost.
- *Missed Trade Opportunity Costs:* This is the cost associated with failure to get orders executed or if the orders are partially filled or if the orders are not filled in a timely manner. In other words, missed trade opportunity cost is the difference between getting the trade at the desired price, and the first next opportunity. So, it is the cost associated with delay in transaction.

In the financial industry, the simplest and commonly used method for calculation of transaction costs is 'Quoted Spreads' (Teschner, 2012). This can be calculated using the trade and order book data. Let us say $Bid_{c,t}$ is the bid price for a contract 'c' at time 't' and $Ask_{c,t}$ is the corresponding ask price for the contract 'c' at time 't'. The mid quote of Mid price of the contract c is denoted as $Mid_{c,t}$. The quoted spread can thus be calculated as:

$$QuotedSpread_{c,t} = \frac{(Ask_{c,t} - Bid_{c,t})}{2 * Mid_{c,t}} \quad (7)$$

The spread paid when executing a market order against a limit order is termed as effective spread. Let us say $Price_{c,t}$ is the execution price then the effective spread can be calculated as:

$$EffectiveSpread_{c,t} = S_{c,t} * \frac{(Price_{c,t} - Mid_{c,t})}{Mid_{c,t}} \quad (8)$$

$S_{c,t}$ denotes the trade side, +1 for a buy order and -1 for a sell order.

The realized spread denotes the revenues of liquidity supplier (Bessembinder and Kaufman, 1997). (Glosten and Milgrom, 1985) model highlights that if the risk of trading against asymmetrically informed traders is high then the spread is wide to compensate the informed traders for their losses. After 'n' minutes of trade execution, the realized spread is calculated as:

$$RealizedSpread_{c,t} = S_{c,t} * \frac{(Price_{c,t} - Mid_{c,t+n})}{Mid_{c,t}} \quad (9)$$

One of the recently proposed spread estimator method which can be used for ISPMs is (Corwin and Schultz, 2012). As all the orderbook data may not be available

or the data availability will be limited in the ISPM, the transaction price method proposed by (Corwin and Schultz, 2012) will be useful. They derived an estimator for the bid-ask spread based on the daily high and low prices. Daily high prices H_p is almost always the execution price of buy order and daily low price L_p is most likely the execution price of a sell order. The price ratio of high-to-low price is due to the volatility which proportionately increases with the length of trading intervals. Hence, they proposed an estimate of a contract's bid-ask spread as a function of the high-to-low price ratio for a single two day period. The high-to-low ratio for two consecutive trading days is ($H_{p,\,p+1}$, $L_{p,\,p+1}$). They defined the spread estimator as:

$$SpreadEstimate = \frac{2(e^{\alpha}-1)}{1+e^{\alpha}} \tag{10}$$

where

$$\alpha = \frac{\sqrt{(2\beta)}-\sqrt{\beta}}{3-2\sqrt{2}} - \sqrt{\frac{\gamma}{3-2\sqrt{2}}} \tag{11}$$

$$\beta = (ln\frac{H_p}{L_p})^2 + (ln\frac{H_{p+1}}{L_{p+1}})^2 \tag{12}$$

$$\gamma = (ln\frac{H_{p,p+1}}{L_{p,p+1}})^2 \tag{13}$$

6.5 Liquidity

Liquidity can be defined as the ability to execute large size orders quickly, at low cost and at any time during the market hours (Harris, 2002). Liquidity is an important market characteristic for market stakeholders. High liquidity allows traders to execute their trades in an efficient and cost-effective manner. Market operators like a liquid market because it attracts many traders to the market, and improves liquidity and information efficiency in the market. Market regulators like liquid markets as the liquid markets are often less volatile than the illiquid markets.

The (Amihud, 2002) illiquidity measure can be used for (il)liquidity measurement in the ISPM. The method uses the daily ratio of absolute returns for a specific contract at a given time, in relation to the trading volume. Let us say that $|R_{ct}|$ represents the return for contract 'c' in the time period 't', and Vol_{ct} represents the trading volume for the contract 'c' in the time period 't', and T_{Di} denotes the number of trading days in that period. The illiquidity for the contract 'c' represented as IL_c is expressed as:

$$IL_c = \frac{1}{T_{Di}} \sum_{t=1}^{T_{Di}} \frac{|R_{ct}|}{Vol_{ct}} \tag{14}$$

Let us say, there is a futures contract listed on ISPM which pays \$1 if a vulnerability is discovered in the biometric authentication system of mobile phone 'M' on or before 'X' date and pays nothing otherwise. If all the traders who do not have any private information and believe that there is 40 percent probability of discovery of vulnerability in the said system and on or before the expiry date, then the price of the contract will be 40 cents.

On the other hand an information security researcher who has some knowledge about the system believes that he can discover a vulnerability before the expiry date, Thus for him the probability of vulnerability discovery is higher than 40 percent. Thus the security researcher believes that the probability of vulnerability discovery stands at 100%, denoted by 'λ'. In this case the security researcher is well informed and no one else has this information. So, when he starts buying contracts starting from 40 cents, he is pushing up the price.

Let us say, that average buy price for the security researcher is represented as:

$$P_{AVB} = 0.4 + \frac{T_c}{L} \tag{15}$$

where P_{AVB} is the average buy price, T_c denotes the total number of contracts purchased, and L is a parameter that characterizes the market liquidity. If the market is very liquid then the security researcher can buy a large number of contracts without significantly affecting the market price.

The number of contracts which the security researcher should buy to maximize his profits depends upon λand L. As the contract pays \$ 1 with probability λ, the expected value of owning the contract is λ. Therefore, the expected value of security researcher's holding is λT_c. The total cost incurred on acquisition of this position stands at $P_{AVB}T_c$. So the expected profit for the security researcher can be represented as:

$$\lambda T_c - (P_{AVB}T_c) = \lambda T_c - (0.4T_c + \frac{T_c}{L})T_c \tag{16}$$

The expression shows that the security researcher with good information can make more money in a liquid market.

6.6 Manipulation Resistance

Manipulation in information security prediction markets can take at least two forms. Firstly, when a trader tries to control the rate of information revelation and decides to temporary trade against the information. A trader who is confident that no one else has the same information may prefer to do several small size trades instead of one big trade. Also, to avoid signaling to other traders, the trader needs to avoid pattern, such as

same order size in his small size trades (Chakraborty and Yilmaz, 2004). This form of manipulation (hiding true information) is relatively less harmful. However, if the trader fears that other traders may also acquire the same information then the trader may actually do a big trade thereby revealing (signaling) the information to other traders.

A second type of manipulation of prices is possible when traders trade in opposite of the information they have and later the trades are not reversed. Traders sometimes do this to create confusion in the market and let the contracts trade at or around a particular price. This type of manipulation can be tackled by limiting the trade limit of traders, so that if they trade against the information they will lose on the trades. Also, if they do not trade quickly on the information they have then other may acquire the same information and trade accordingly thereby deepening the losses for those who did not trade or traded in the opposite direction. Researchers have studied various models of financial market microstructure with consideration of various types of noise traders such as those who trade randomly, traders who have manipulate the closing price for higher futures market settlement, traders who need immediate liquidity, and traders who have quadratic preferences over the current market price (Kumar and Seppi, 1992; Hillion and Suominen, 2004; Hanson et al., 2006).

These studies have proved that manipulators are just another type of noise traders and in effect they improve the price accuracy. A trader seeking to manipulate the prices has hidden bias towards the direction and extent to which he intends to manipulate the price. Other traders participating in the market are expected to have average bias. When the manipulator's bias and average trader bias is exactly equal then the markets perform as if there is no price manipulation. On the other hand, if the manipulator bias is lower or higher than the average bias then this will be reflected in market prices. However, speculators competition leads to correction in average price and the price accuracy is not affected with manipulative noise trading. The studies based on market data confirms the theory that average price accuracy is not affected by manipulators. Though there has been one case of successful manipulation (Hansen et al., 2004) but others have reported that manipulators have not been successful in decreasing the price accuracy, in the field (Camerer, 1998), historically (Rhode and Strumpf, 2004), and in the laboratory (Hanson et al., 2006).

The evidence that noise trading generally leads to increase in market accuracy suggests that there is little to worry about price manipulation attempts in the information security prediction markets. As long as the traders with correct information and rational behavior outnumber the manipulators in terms of trading size, the net effect will lead to increase in average price accuracy. In other words, the impact of price manipulation in information security prediction market will depend upon the financial muscles of the manipulator.

7 CONCLUSIONS AND FUTURE WORK

In this article, we identified a set of design requirements for the ISPM. We explained three types of contracts: binary, index, and spread. Also, we explained the importance of clear and unambiguous specification of contracts. We explained four different types of trading mechanisms, CDA, CDAwMM, DPM, and MSR. The trading mechanisms are compared on the four criteria: continuous incorporation of information, liquidity guarantee, bounded risk to market operator, and cash out option during the market hours. The specific features of the trading mechanisms can be used to design contracts to achieve the specific objectives. We explained the significance of clearing house in settlement of trading contracts, counterparty risk management, role of trusted third party, and as a custodian of confidential information and intellectual property. Also, we identified several types of traders who are expected to participate in ISPM. Also, trader's motivation and incentives for the participation is explained. The importance of market regulation and specific legal permissions is briefly discussed. Furthermore, we identified six performance measures for ISPM: Information elicitation, Transparency, Efficiency, Transaction Cost, Liquidity, and Manipulation resistance. We explained these individual factors in the light of information security specific objectives of the prediction market.

In future, we intend to design, demonstrate and evaluate some financial contracts to address a particular type of security risks. Then, we plan to demonstrate a complete design and model of risk hedging in an information security prediction market.

REFERENCES

Amihud, Y. (2002). Illiquidity and stock returns: cross-section and time-series effects. *Journal of Financial Markets*, 5(1):31–56.

Berg, J. E. and Rietz, T. A. (2003). Prediction markets as decision support systems. *Information Systems Frontiers*, 5(1):79–93.

Bessembinder, H. and Kaufman, H. M. (1997). A cross-exchange comparison of execution costs and information flow for NYSE-listed stocks. *Journal of Financial Economics*, 46(3):293–319.

Camerer, C. F. (1998). Can asset markets be manipulated? a field experiment with racetrack betting. *Journal of Political Economy*, 106:457–482.

Chakraborty, A. and Yilmaz, B. (2004). Manipulation in market order models. *Journal of Financial Markets*, 7(2):187–206.

Corwin, S. A. and Schultz, P. (2012). A simple way to estimate bidask spreads from daily high and low prices. *Journal of Finance*, 67(2):719–760.

EOG (2006). Tradesports' bad call. *http://forums.eog.com/showthread.php/39353-Tradesports-Bad-Call*.

Fama, E. F. (1970). Efficient capital markets: A review of theory and empirical work. *The Journal of Finance*, 25(2):383–417.

Fidler, M. (2014). *Anarchy of Regulation: Controlling the Global Trade in Zero-Day Vulnerabilities*. PhD thesis, Stanford University.

Glosten, L. R. and Milgrom, P. R. (1985). Bid, ask and transaction prices in a specialist market with heterogeneously informed traders. *Journal of Financial Economics*, 14(1):71–100.

Google (2014). Projectzero. *http://googleprojectzero.blogspot.be/*.

Hansen, J., Schmidty, C., and Strobelz, M. (2004). Manipulation in political stock markets - preconditions and evidence. *Applied Economics Letters*, pages 459–463.

Hanson, R. (2003). Combinatorial information market design.

Hanson, R. (2006). Designing real terrorism futures. *Public Choice*, 128(1-2):257–274.

Hanson, R., Oprea, R., and Porter, D. (2006). Information aggregation and manipulation in an experimental market. *Journal of Economic Behavior & Organization*, 60(4):449–459.

Harris, L. (2002). *Trading and exchanges: Market microstructure for practitioners*. Oxford University Press.

Hillion, P. and Suominen, M. (2004). The manipulation of closing prices. *Journal of Financial Markets*, 7(4):351–375.

Johannesson, P. and Perjons, E. (2014). *An Introduction to Design Science*. Springer International Publishing, 1 edition. ISBN: 978-3-319-10631-1.

Kumar, P. and Seppi, D. J. (1992). Futures manipulation with cash settlement. *The Journal of Finance*, 47(4):1485–1502.

Luckner, S. (2008). Prediction markets: Fundamentals, key design elements, and applications. *The 21st Bled eConference, eCollaboration: Overcoming Boundaries Through Multi-Channel Interaction*.

Pandey, P. and Snekkenes, E. (2014a). Applicability of prediction markets in information security risk management. In *Database and Expert Systems Applications (DEXA), 2014 25th International Workshop on*, pages 296–300.

Pandey, P. and Snekkenes, E. (2014b). Using prediction markets to hedge information security risks. In Mauw, S. and Jensen, C., editors, *Security and Trust Management*, volume 8743 of *Lecture Notes in Computer Science*, pages 129–145. Springer International Publishing.

Pennock, D. M. (2004). A dynamic pari-mutuel market for hedging, wagering, and information aggregation. In *In Proc. of the 5th ACM Conf. on Electronic Commerce*, pages 170–179.

Plott, C. R. and Chen, K.-Y. (2002). Information Aggregation Mechanisms: Concept, Design and Implementation for a Sales Forecasting Problem. W.P. 1131, California Institute of Technology.

Rhode, P. W. and Strumpf, K. S. (2004). Historical presidential betting markets. *The Journal of Economic Perspectives*, 18(2):127–141.

Spann, M. (2002). *Virtuelle Börsen Als Instrument Zur Marktforschung*. Deutscher Universitäts-Verlag.

Sripawatakul, P. and Sutivong, D. (2010). Decision framework for constructing prediction markets. In *The 2nd IEEE Int. Conf. on Information Management and Engineering (ICIME), 2010*.

Teschner, F. (2012). *Forecasting Economic Indices Design, Performance, and Learning in Prediction Markets*. PhD thesis, Karlsruher Institut fr Technologie.

TradeSports (2015). Tradesports. *https://www.tradesports.com/*.

WEF (2014). Global risks 2014. Insight Report 9th Edn., No.: 090114, World Eco. Forum, Geneva.

Weinhardt, C. and Gimpel, H. (2007). Market engineering: An interdisciplinary research challenge. In Jennings, N., Kersten, G., Ockenfels, A., and Weinhardt, C., editors, *Negotiation and Market Engineering*, number 06461. IBFI, Germany.