Understanding the Issues in Quantification and Management of Information Security Risks

Ritesh Kumar Tiwari
Center for Data Engineering,
International Institute of Information Technology,
Hyderabad, India
ritesh@students.iiit.net

Kamalakar Karlapalem
Center for Data Engineering,
International Institute of Information Technology,
Hyderabad, India
kamal@iiit.net

ABSTRACT

One of the areas that have been *Archilles Heel* of information security community is inability to efficiently quantify the security risks associated with a system (or network as a whole). A major hurdle is that we do not understand completely the nature of causes for IT security risks. We strongly believe that security risks will be poorly understood until a much better job of quantification of losses from security breaches is done. In order to protect themselves from security breaches, organizations are making ample investments, but still they are vulnerable to attacks. Since achieving perfect security is monetarily and practically infeasible, adoption of risk management concepts for making cost effective tradeoffs in pursuit of security goals is inherently necessary. This paper analyzes various issues related to holistic organization wide quantification and management of security risks.

Categories and Subject Descriptors

H.1.0 [**Information Systems Applications**]: Models and Principles; D.2.0 [**Software Engineering**]: Management—*General*

General Terms

Security, Risk Analysis

Keywords

Risk Analysis, Risk Quantification, Attacks

1. INTRODUCTION

Information security is important in proportion to an organization's dependence on information technology. Security of a computer based information system should protect the *Confidentiality, Integrity* and *Availability* (*CIA*) aspects of the system. From an organizational centric view, loss of information could lead to *Direct losses* (quantified in terms of dollar losses) and *Indirect losses* (e.g. loss of customer faith[1], damage to reputation etc.). As Blakley et.al.[1] points out, the basic problem with information security is that it focuses more on reducing the probability of occurrence of an adverse event, rather than on reducing its consequences. *So the main aim of any security risk management technique should be to minimize the cost of risk to business, rather than on minimizing the probability of occurrence of adverse event.*

Quantifying risks helps in determining the losses incurred if the threat (i.e. exploiting a vulnerability) is materialized by attacker. If the quantified risk is much above acceptable threshold, then the organization has to invest in appropriate countermeasures so as to decrease the value at risk. Exploiting a vulnerability V_i incurs attacking cost $cost_A(V_i)$ to attacker. Usually a rational attacker will not prefer to attack a target unless:

1. The return value R_A of attack is much more than the attacking cost, i.e. $ret_A(V_i) \gg cost_A(V_i)$, and
2. Probability that an attack attempt (att) targeting vulnerability V_i $\big($i.e. $p\ (att(V_i))\big)$ being successful is high (otherwise it will accrue attacking cost to attacker with zero returns).

Accurately measuring the attack cost borne by attacker is a challenging task because we cannot deterministically infer the attackers *intention, objectives* from partial attack events (i.e. ongoing attack) and the *strategies*[2] that he will be employing further so as to succeed in his task. There may exist many avenues to launch an attack against a specified target. Usually an attacker will choose a path that incurs low cost, high probability of success and low chances of detection.

In order to protect itself from vulnerability V_i targeting resource R_j, defender has to implement safeguard S_k and this incurs investment cost $C_D^{S_k}(V_i)_{R_j}$ to defender. The aim of defender in implementing safeguard S_k is to reduce probability of attack by maximizing cost borne by attacker (approximate value) so that it becomes monetarily unattractive for attacker to launch an attack. As evident from above, security strength metrics gauge security from an adversary's perspective, whereas security risk metrics measure security from

[1]Many customers now days hesitate in responding to promotional e-mails due to fear of Phishing Attacks.

[2]In case of manual penetration attacks, the next action that attacker will take depends on the outcome of previous actions.

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. To copy otherwise, to republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee.
NSPW'2005 California, USA
Copyright 2005 ACM X-XXXXX-XX-X/XX/XX ...$5.00.

defenders perspective. An efficient risk mitigation strategy should incorporate both these metrics for identifying potential risk factors and selecting safeguards for mitigating risks arising from those factors.

2. PREVIOUS WORK

Gordon et.al.[2] propose an economic model that determines the optimal amount to invest for protecting confidentiality, availability, authenticity, non-repudiation and integrity of information. They use a version of ALE (annual loss expectancy) that is modified for situations where at most one successful breach will occur. Kevin Soo Hoo[3] uses safeguard efficacy to weight the benefits of different security policies. Formally speaking, net benefit for K^{th} security policy P_k is defined as:- $Net\ Benefit_k = (ALE_0 - ALE_k) + Added\ profit_k - Added\ cost_k$. The main limitation of this model is its over estimation in risk reduction in case of using those safeguards, which substitutes each other in functionality. Schechter[4] in his doctoral dissertation develops a formal model for economic measure of software security strength with respect to threat scenarios. He also proposed a regression and probabilistic framework for anticipating new threats. Meadows[5] proposed cost based framework based on attack cost and protocol engagement cost for resisting denial of service attacks against protocols. Jelen et. al.[6] discuss the role of assurance in risk management with emphasis on uncertainty in risk measurement. Blakley et.al.[1] gives an overview of conventional risk management mechanism like *liability transfer, Indemnification* (pooling and hedging), *mitigation,* and *retention* that are used routinely by businesses. The aim of an effective risk management strategy should be that *given a fixed budget, what action plans should be selected so that the residual aggregated information security risk is minimized to an acceptable level.* Lenstra et.al.[7] proposed a quantitative model to assess and aggregate information security risks. The authors propose to use multiple choice knapsack problem which is equivalent to risk mitigation under budget constraint problem for finding out an effective risk mitigation strategy. The main disadvantage of proposed model is that it will not give effective aggregated risk measure for those attacks which substantially effect the confidentiality, integrity and availability of information simultaneously.

Farahmand et.al.[8] analyzes various aspect of security risk assessment and propose a risk management model to effectively mitigate risks. Butler[9] proposes a cost-benefit analysis method *SAEM* using which security design alternatives are compared with organization current selection of security techniques to determine if a more cost effective solution is possible. The pitfall of the approach is that SAEM can only evaluate technological design choices and not risk mitigation choices. Schechter[10] proposes an economic model of security risk and discusses factors that affect attack and breach rates. Cremonini et.al.[11] propose to couple the Return on Investment - ROI (from defender point of view) with Return on Attack - ROA (from attacker point of view) so that better judgments for selecting safeguards can be made. Achieving perfect security is practically infeasible for an organization. So organization has to prioritize critical resources that need to be saved from identified risks and make appropriate tradeoffs in making investment for deploying safeguards so that overall security goal is achieved. Tiwari et.al.[12] analyze such tradeoffs from perspective of Worm/ Denial of Service attacks, Insider/ Outsider attacks, and Penetration attacks.

2.1 Symbols used

We have used following symbols throughout the paper-

$vect_t^S$	Security vector at time t
$C_A^{S_K}(V_i)_{R_j}$	Cost borne by attacker for exploiting resource R_j using vulnerability V_i after safeguard S_k is enforced
$C_D^{S_k}(V_i)_{R_j}$	Cost borne by defender for protecting R_j from V_i using S_k
$ret_A(V_i)_{R_j}$	Return value of attack for attacker exploiting R_j using V_i

3. PROBLEM MOTIVATION

As *CRA grand challenge*[13] number three points out, "*we cannot effectively manage the risk if we cannot measure the risk*". For having an efficient risk management strategy, the measures should be consistent, unbiased and unambiguous. Factors which hinders accurate quantification of information risk are-

1. Failures in networked system are not independent, but depends on many factors spanning throughout the organization. The risk that information system faces is dynamic as it depends upon various attack patterns and vulnerabilities which evolve with time.

2. Sufficient data on likelihood and attack patterns is not available. Even we do not understand full nature of causes that creates information security risks and the emergent behavior of vulnerabilities in information systems.

3. We cannot accurately infer attacker objectives (i.e. how valuable the target is for him? etc.) and strategies that he follows during an attack.

Four parameters that have to be evaluated for designing an effective information security risk mitigation strategy are-

1. Identify critical risks that the organization information system faces, and estimate the approximate consequences that organization has to bear if the threat is materialised in reality.

2. Quantify investment cost borne by defender for implementing and maintaining safeguards to mitigate risks.

3. Quantify (approximately) attacker cost borne by attacker for launching an attack

4. Synergistically consider both defender cost and attacker cost for designing risk mitigation strategy so that we can maximize attacker cost with minimum (optimum) investment by defender.

3.1 Preliminaries

When an attack is launched by rational attacker, his intent is to simply maximize his incentives. Based on economic theory, such incentives can be categorized as money, emotional reward and fame. After an attack is successful, the incentives earned by attacker depend on the degradation of

specific set of elements in security vector. For simplicity, we will consider confidentiality, integrity and availability as elements of security vector (based on scenario under consideration, authentication and non-repudiation can also be considered as metric elements). The incentives earned by attacker for an attack that starts at time t_1 and ends at t_2 can be measured in terms of degradation (vec_{t_1}, vec_{t_2}) which is basically the distance between security vectors. The aim of risk management strategy is to minimize the degradation of security vector by implementing safeguards S_k so that return value $ret_A(V_i)_{R_j}$ is much less than the cost borne by attacker for launching attack, i.e.
$C_A(V_i)_{R_j} \ll ret_A^{S_k}(V_i)_{R_j} \ll C_A^{S_K}(V_i)_{R_j}$

4. DIMENSIONS OF INFORMATION SECURITY RISKS

Information security risks can be measured in three dimensions. They are- *cost to defend*, *cost to attack*, and *time*.

4.1 Cost to Defend

Cost to Defend refers to cost borne by defender in protecting security vector elements of resource R_j (i.e. $C_D^{S_k}(conf, int, avail)_{R_j}$). This cost is an aggregate of cost incurred on implementation and maintenance of safeguard S_k. First the defender should identify the consequences that he will have to bear if a security breach takes place and should preferably quantify (if not possible, then qualify) the losses that he will have to bear because of compromise of each security vector element.

$$Expected\, loss_{Breach_D}^{per\ event} = Loss_D^{quant}(conf)_{R_j} + Loss_D^{quant}(int)_{R_j} + Loss_D^{quant}(aval)_{R_j} + Loss_D^{qual}(conf)_{R_j} + Loss_D^{qual}(int)_{R_j} + Loss_D^{qual}(aval)_{R_j}.$$

Here *quant, qual* represent quantitative and qualitative evaluation whereas *conf, int, aval* represents confidentiality, integrity and availability elements of security vector. The expected loss contain both quantified security loss (e.g. monetary consequences organization has to bear) and qualified non monetary loss (e.g. customer faith). It should be noted that here we are treating confidentiality, integrity and availability as independent parameters. It is feasible to further develop this model where it is not so. In such cases, cost model can get fairly complex. Similarly the notions of quantitative and qualitative cost are good mechanisms to distinguish between tangible and intangible cost. Sometimes intangible cost might be prohibitively high and overshadow comparatively negligible tangible costs. Quantified losses can be aggregated based on approximate frequency of attack so as to determine total value at risk, and hence to decide whether threat is critical and therefore safeguards has to be deployed or not.

$$Total\, loss_{Breach_D} = Expected\, loss_{Breach_D}^{per\ event} \times event\ frequency$$

The qualified losses corresponding to security vector elements cannot be aggregated, but are practically very useful when selection of safeguards is made based on how efficiently it is going to protect individual vector element from a particular threat. Based on the value at risk corresponding to individual element of security vector, appropriate safeguard is selected which focuses more on those vector elements with high value at risk than as compared to other elements. Example, for a company storing credit card transaction database of an e-commerce site, confidentiality of database is very important and not its availability to customers (because database will be accessible only to authorized personals from e-commerce site and not customers). So more investment should be done in implementing computationally extensive authentication system and maintaining access logs, as compared to purchasing bandwidth for availability.

If an enterprise has deployed safeguard S_k to protect R_j from V_i, and the safeguard proves to be ineffective in stopping attacks exploiting vulnerability V_i, then losses borne by defender will be equal to *summation* of *expected loss*, *cost of safeguard* $C(S_k)$, and *interest* that organization would have earned by investing $C(S_k)$ in other ventures.

$$Expected\ loss_{Breach_D}^{(S_k=fail)} = \{Expected\ loss_{Breach_D}^{per\ event} + C(S_k) + Interest\ (C(S_k))\}$$

Example 1. Suppose for a recently discovered vulnerability, the administrator applies a patch and the patch doesn't work as intended but creates configuration errors in the system and finally the organization becomes victim of attack. In this case, the cost borne by organization is not only the consequence of security breach, but also the cost of applying patch (in terms of system downtime and hence the productivity loss) and cost of tweaking up configuration errors. Beattie et.al.[14] discuss such issues in detail.

4.2 Cost to Attack

In order to successfully exploit vulnerability V_i on resource R_j, an attacker has to execute series of steps[3] $\{E_1^{att}, E_2^{att}, \ldots, E_{i-1}^{att}\}$ exploiting vulnerabilities $\{V_1, V_2, \ldots, V_{i-1}\}$ on resources $\{R_1, R_2, \ldots, R_{j-1}\}$ respectively. The motive behind an attack is to compromise one or more elements of security vector on target resource. The cost of individually exploiting these vulnerabilities is given by-

$$C(E_1^{att}(V_1)_{R_1}),\ C(E_2^{att}(V_2)_{R_2}),\ \ldots,\ C(E_{i-1}^{att}(V_{i-1})_{R_{j-1}}).$$

Let probability of detection P_{detect} for each of these events be-

$$P_{detect}(E_1^{att}(V_1)_{R_1}),\ \ldots,\ P_{detect}(E_{i-1}^{att}(V_{i-1})_{R_{j-1}})$$

There may exist multiple avenues to launch an attack against a target. For example,

$$E_1^{att}(R_1)_{V_1} \prec E_4^{att}(R_4)_{V_4} \prec \ldots \prec E_{i-2}^{att}(R_{i-2})_{V_{i-2}}$$

and

$$E_2^{att}(R_2)_{V_2} \prec E_3^{att}(R_3)_{V_3} \prec \ldots \prec E_{i-1}^{att}(R_{i-1})_{V_{i-1}}$$

represents two possible attack paths where $\prec$ denotes partial causal relationship between events.

Fundamentally cost of attack path, i.e.

$$C(E_1^{att}(V_1)_{R_1}) + C(E_4^{att}(V_4)_{R_4}) + \ldots + C(E_{i-2}^{att}(V_{i-2})_{R_{j-2}})$$

[3]May be on same resource or on stepping stones.

(for path 1) and probability of detection -

$$\left[\ P_{detect}(E_1^{att}(V_1)_{R_1}),\ P_{detect}(E_4^{att}(V_4)_{R_4}), \ldots \right.$$
$$\left. ,\ P_{detect}(E_{i-2}^{att}(V_{i-2})_{R_{j-2}})\right]$$

along various steps in attack path are two fundamental metrics on which an attacker will take decision to select particular path to attack. The attack cost can be further subcategorized into two domains-

1. *Monetary cost* of hardware, software, bandwidth, time etc. that an attacker has to invest for launching attack, and
2. *Non monetary cost* such as risk of prosecution.

Usually rational attacker will select a path with overall low monetary attack cost[4] and low probability of detection[5] (especially during last phases of attack).

4.3 Timeline

Information security risk that an organization faces is a dynamic quantity and depends not only on local factors (within an organization) but also on temporally varying global factors. As far as information security is concerned, an attacker evaluates his potential gains in global context. So organizations should consider both local and global context of a threat while making risk mitigation decisions.

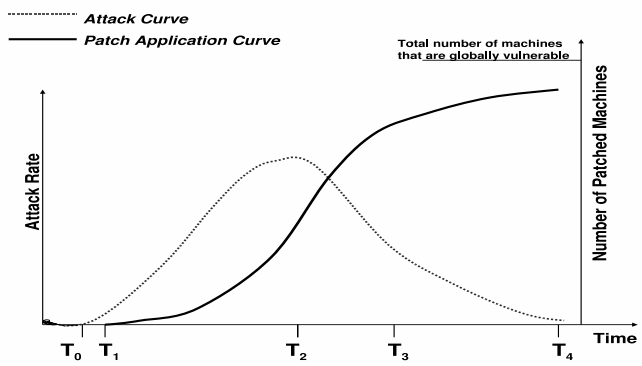

Figure 1: Relationship between attack rate and patch application rate

Example 1. As shown in fig.1, the probability of attack (derived from attack rate) and hence the risk that organization faces from attack targeting vulnerability V_i on security vectors of resource R_j first increased with time (from T_0 to T_2) after the vulnerability is discovered (T_0) and patch is rolled out (T_1). Later on as the number of patched machines increases continuously, the attack curve starts receding and slowly drops to a negligible value.

Example 2. Consider a system which store tenders filed by various organizations for a project. The security risk that system faces is towards confidentiality and integrity of tenders already submitted, and will remain fixed till the tender value is publicly disclosed. After public disclosure, the system has zero risk level.

As evident from above, the time dependent variation of risk depends upon scenario under consideration and is not a general concept.

5. ISSUES RELATED TO INFORMATION SECURITY RISK MANAGEMENT

Issue such as what is the most cost effective way to contain the risk, where to spend, and what percent of total budget should be spent for a particular threat are considered to be as hot topics of information security risk management. In this section, we analyze these core issues that encompass the field of security risk management.

5.1 Aggregated risk *vs.* Residual Operational Risk

An organization consist of n business processes (pr_i where $i = 1$ to n) running in synergy to achieve business goals. Each business process is exposed to certain amount of *current security risk*[6] with consequent losses.

$$Consequent\ Loss\ =\ \Big(\ Expected\ Loss_{breach}(pr_i)\ \times\ frequency_{breach}(pr_i)\Big)$$

Here $frequency_{breach}(pr_i)$ represents how frequently is business process pr_i targeted by attackers. Each business process can be used by one or more applications. So the *aggregated security risk* that organization faces is the *summation* of *current security risk* of all business processes.

$$Aggregated\,Security\,Loss\ =\ \sum_{i=1}^{n}\Big(\ frequency_{breach}(pr_i)\ \times\ k_i \times Expected\,Loss_{breach}(pr_i)\Big)$$

Here k_i denotes the number of critical applications in which business process pr_i is used. In order to design an effective risk mitigation strategy, those business processes which contribute more in security risks having severe consequences for the organization should be identified. For every threat, there are numerous mitigation safeguards (S_j) with varying cost and degrees of effectiveness. Some of these safeguards may even overlap in threat coverage (i.e. protecting more than one element of security vector).

One aim of security risk management is to select those risk mitigation safeguards so that *aggregation* of *residual security risk* is minimized.

$$Aggregate\ Residual\ Security\ Loss\ =$$
$$\exists j\ \sum_{i=1}^{n}\Big(\ frequency_{breach}^{S_j}(pr_i) \times k_i \times Expected\,Loss_{breach}(pr_i)\Big)$$

A safeguard is said to be effective when-

$$\Big(\ frequency_{breach}^{S_j}(pr_i)\ \ll\ frequency_{breach}(pr_i)\Big).$$

Ideally, $frequency_{breach}^{S_j}(pr_i)\ =\ 0$. The *residual risk* (or op-

[4]In case of worm attacks, the monetary cost is insignificant for attacker because this cost is borne by system which has been breached by worm.

[5]In case of insider attacks, non monetary cost (like probability of detection) is very significant because it is the risk of being detected and prosecuted which hinders an insider from launching an attack.

[6]Here we have referred term *risk* and *loss* synergistically because every risk has an associated loss if that risk is materialized in reality.

erational risk) after implementing the safeguard S_j should be much below the threshold level. The effectiveness of a risk mitigation strategy can be found by-

$$\left(\frac{Aggregate\ Security\ Risk\ -\ Aggregate\ Residual\ Security\ Risk}{Aggregate\ Security\ Risk}\right) \times 100$$

5.2 Cost to Defend *vs.* Cost to Attack

As per theory of economics, a rational attacker will not attack a target unless the return that he gets from successful attack is more than the efforts (attack cost) that he puts into for attack, i.e., $\left(Ret_A(V_i)_{R_j} \gg C_A(V_i)_{R_j} \right)$. The reward that an attacker will get is given by -

$$Reward_A(V_i)_{R_j} = Ret_A(V_i)_{R_j} - C_A(V_i)_{R_j}.$$

In practical scenarios, attacker usually exploit many resources $(R_1, R2, \ldots, R_j)$ and then use them as stepping stone for launching assault on final target resource R_j. In this case, the cumulative cost of attack is given by -

$$\Big(Cumulative\ Cost = C_A(V_1)_{R_1} + C_A(V_2)_{R_2} + \ldots + C_A(V_{i-1})_{R_{j-1}} + C_A(V_i)_{R_j} \Big).$$

The reward that an attacker gets from such an attack consisting of series of exploitations is given by -

$$Total\ Reward = \exists i\ \forall_j \left(Ret_A(V_i)_{R_j} - C_A(V_i)_{R_j} \right).$$

Here by $(\exists i\ \forall_j)$ we mean that from a set of vulnerabilities (i), attacker can use any vulnerability $(\exists i)$ to exploit resource R_j subjected to various constraints as discussed previously. Motto of safeguard focusing on security vector elements whose compromise results in high consequences is to effectively make the total return value of attack less than zero for attacker, i.e.

$$\left[\exists i\ \forall_j \left(Ret_A(V_i)_{R_j} - C_A(V_i)_{R_j} \right) \ll 0 \right].$$

An effective research direction in this regard is to design techniques so that cost of exploitation of series of resources increases monotonically as number of resources in exploit chain increases, thereby monotonically decreasing the reward value of attack to attacker.

From an economic theoretic perspective, defender will not invest more money in safeguards than the value of resource that he trying to protect. Schechter et.al.[15] discuss such issues in terms of value of *loot* (resource) versus probability of being caught and cost of attack borne by thief. Here the term *value of resource* is vague and difficult to be quantified. Attack graph based hardening techniques as described by Noel et.al.[16] can be used to find value of target. It is quite probable that resource connected to large number of attractive targets is a prime target of attackers, so that it can be used as stepping stone. *So even if the value of this resource* (in terms of direct consequences resulting from breach that an organization has to bear) *is low, then also organization should invest sufficiently in protecting such resource, because hardening such a resource will harden attack path to all attractive targets to which resource has links to.*

Another open area of research is given a resource R (like Intrusion Detection System or Honeypot) or safeguard S, then at what point across the organization should they be placed/ implemented so that it results in more accurate detection/ mitigation of attacks.

6. DIRECTIONS FOR FUTURE RESEARCH

The relationship between security policies and risk analysis is by their very nature complex. Security policies set the boundaries of acceptability across the organization, whereas risk analysis determines what controls (and expenditures) are appropriate for specific area/ systems/ applications. So research directed towards reducing complexity between security policy and risk analysis is needed so that better assurance can be made for designing new security policy from existing policy.

As discussed in section 4.1, when a patch is applied, we don't know whether the patch will work correctly or not. If patch doesn't function correctly, then it has to be removed and this incurs cost on defender. So we need mechanisms which can be used to evaluate effectiveness of security mechanisms proposed by risk analysis module without subjecting the business process system to higher level of risk. Blakley et.al.[1] urged the need to develop "*secure mouse analog*" for use as an test-bed for security measures as has been done on real mouse and monkeys by pharmaceutical companies. Lack of standards for quantifying potential cost of computer security incidents is also a major problem for management of information system risks.

Theory of *Uncertainty Quantification* (*UQ*)[17] defines *UQ* as quantitative characterization and use of uncertainty in information applications. There are basically two different kinds of uncertainties-

1. Variability
2. Lack of Knowledge

For accurate risk quantification, we need to have accurate insight (good knowledge) into *variability of losses* (distribution function) and *value at risk*. Collecting enough data to determine distribution function underlying the behavior of certain information security threat is practically infeasible given the fast and constantly changing nature of information security threats. Notable examples are *heavy tailed distributions* where high impact event occurs with very low probability. So an area of research is how to make efficient risk management decisions even if data is *sparse*, *incomplete*, and *incorrect*. We strongly believe that *fuzzy logic* can play a vital role in this regard. Some preliminary discussion on use of fuzzy logic for risk analysis has been published in [20, 21].

Another interesting area of research is to develop risk analysis and mitigation strategy that incorporate notion of *temporally dynamic trust*. Human beings manage risk in terms of mutual trust between one another which is time variant. Systems that incorporate notion of time varying trust will probably fall in category of attack tolerant systems (i.e. critical services will keep on running even during an attack). Another challenge that arises in designing such systems is how to measure the degree of assurance and survivability of a given system for given environment and application domain.

Various formal verification tools like NRL Protocol Analyzer (by Naval Research Laboratory) and $Mur\varphi$ (by Stanford University) etc. have been developed for automated

formal verification of cryptographic protocols. Since real world risk analysis is both computationally complex and intensive, need of such automated tools that allows reasoning on attacks and helps in building security decisions is highly desirable. An algebraic approach for modeling risk management projects and proving properties in risk management signature has been proposed by Hamdi et.al.[23]. So the challenge is to design an *automated*, *immune* (i.e. resistant to attack and faults) risk analysis system which is not vulnerable to attack from privileged malicious insiders.

We believe that *Economics of Information Security* is pretty different from traditional economic theory. Many laws of traditional economic theory are not applicable when we try to analyze security economics from global context (from point of view of both attacker and defender). So active research should be directed in field of *Securonomics* (i.e. security economics).

Very often, issues has been raised on *ethics* of risk management. Since information security risk management also deals with critical nationwide information infrastructure, so ethics automatically come into consideration. For example, considerations like how much should be invested to mitigate terrorist attack on nationwide critical information infrastructure, whether investment tradeoffs should be made or not etc. frequently arise. We believe that since such infrastructures have direct consequence on human life, so tradeoffs should not be considered in protecting these infrastructures. We strongly believe that risk to human life cannot be quantified. India is fighting against terrorist attacks since last two decades, where tens of thousands of innocent people have been mercilessly killed or rendered homeless. Though it is possible to quantify the consequence of these terrorist attacks in terms of loss of revenue from tourists, amount of military expenditure etc., but it is impossible to quantify the cost of life of innocent citizens.

7. CONCLUSIONS

In order to efficiently manage the risk, we should be able to accurately measure the risk. Today we have no way to differentiate whether a software (system or safeguard) costing $1000 better suits our needs or as software (safeguard or system) costing $2000. We have no metrics to accurately determine the return value of investment that we are making for securing the information. This paper focuses on these problems and proposes an approach based on *security vector elements* to judge protection level that a new system (or safeguard) provides. This paper gives a preliminary approach to tackle this problem, and we are investigating the proposed approach in real life scenarios. Although some additional computational cost is attached with this fine grained analysis of risks, but the results are more accurate, which overshadows the computational penalty. We are looking forward to work in this area so that more accurate methods which provide higher assurance in risk analysis can be developed.

8. REFERENCES

[1] Bob Blakley, Ellen McDermott, and Dan Geer. Information security is information risk management. In *Proceedings of the 2001 workshop on New security paradigms*, pages 97–104, New York, NY, USA, 2001. ACM Press.

[2] Lawrence A. Gordon and Martin P. Loeb. The economics of information security investment. *ACM Trans. Inf. Syst. Secur.*, 5(4):438–457, 2002.

[3] Kevin J. Soo Hoo. *How Much is Enough? A Risk Management Approach to Computer Security.* Ph.D. Thesis, Stanford University, 2000.

[4] Stuart E. Schechter. *Computer Security Strength and Risks: A Quantitative Approach.* Ph.D. Thesis, Harvard University, 2004.

[5] Catherine Meadows. A cost-based framework for analysis of denial of service networks. *Journal of Computer Security*, 9(1/2):143–164, 2001.

[6] G. F. Jelen and J. R. Williams. A practical approach to measuring assurance. In *ACSAC*, 1998.

[7] Arjen K. Lenstra and Tim Voss. Information security risk assessment, aggregation, and mitigation. In *ACISP*, volume 3108 of *Lecture Notes in Computer Science*, pages 391–401, 2004.

[8] Fariborz Farahmand, Shamkant B. Navathe, Philip H. Enslow, and Gunter P. Sharp. Managing vulnerabilities of information systems to security incidents. In *5th International conference on Electronic commerce*, pages 348–354. ACM Press, 2003.

[9] Shawn A.Butler. Security attribute evaluation method: a cost-benefit approach. In *22nd ACM International Conference on Software Engineering*, pages 232–240, 2002.

[10] Stuart E. Schechter. Toward econometric models of the security risk from remote attacks. *IEEE Security & Privacy Magazine*, 3(1):40–44, February 2005.

[11] Marco Cremonini and Patrizia Martini. "evaluating information security investment from attackers perspective: the return-on-attack (roa)". In *Workshop on Economics of Information Security, Harvard University.*, Harvard University, USA, 2005.

[12] Ritesh Kumar Tiwari and Kamalakar Karlapalem. Cost based tradeoffs for information security assurance. In *Workshop on Economics of Information Security*, Harvard University, USA, 2005.

[13] CRA Grand Research Challenges in Information Security and Assurance http://www.cra.org/Activities/grand.challenges/security/home.html.

[14] Steve Beattie, Seth Arnold, Crispin Cowan, Perry Wagle, Chris Wright, and Adam Shostack. Timing the application of security patches for optimal uptime. In *USENIX 16th Systems Administration Conference*, 2002.

[15] Stuart E. Schechter and Michael D. Smith. How much security is enough to stop a thief? the economics of outsider theft via computer systems and networks. In *Seventh International Financial Cryptography Conference*, 2003.

[16] Steven Noel, Sushil Jajodia, Brian O'Berry, and Michael Jacobs. Efficient minimum-cost network hardening via exploit dependency graphs. In *Annual Computer Security Applications Conference*, pages 86–95, 2003.

[17] John Haigh. Probabilistic risk analysis: Foundations and methods. *Journal of the Royal Statistical Society: Series D (The Statistician)*, 52(2):236, 2003.

[18] Ross J. Anderson. Why information security is hard-an economic perspective. In *ACSAC*, pages 358–365, 2001.

[19] Hilary H. Hosmer. Security is fuzzy!: applying the fuzzy logic paradigm to the multipolicy paradigm. In *Proceedings on the 1992-1993 workshop on New security paradigms*, pages 175–184, 1993.

[20] Gerardo Canfora and Luigi Troiano. Dealing with the "don't know" answer in risk assessment. In *ICEIS (2)*, pages 229–237, 2003.

[21] Valentina Casola, Massimiliano Rak, Rosa Preziosi, and Luigi Troiano. Security level evaluation: Policy and fuzzy techniques. In *International Conference on Information Technology: Coding and Computing (2)*, 2004.

[22] F. Harmantzis and M. Malek. Security risk analysis and evaluation. In *IEEE International Conference on Communications*, pages 1897–1901, 2004.

[23] Mohamed Hamdi and Noureddine Boudriga. Algebraic specification of network security risk management. In *Proceedings of the 2003 ACM workshop on Formal methods in security engineering*, pages 52–60. ACM Press, 2003.

[24] G. F. Jelen. A new risk management paradigm for infosec assessment and evaluations. In *ACSAC*, pages 261–267, 1995.

[25] Howard Kunreuther and Geoffrey Heal. Interdependent security: The case of identical agents. In *National Bureau of Economic Research Working Paper - 8871*, 2002.

[26] Gurpreet Dhillon and Steve Moore. Computer crimes: theorizing about the enemy within. *Computers & Security*, 20(8):715–723, 2001.

[27] Peng Liu, Wanyu Zang, and Meng Yu. Incentive-based modeling and inference of attacker intent, objectives, and strategies. *ACM Trans. Inf. Syst. Secur.*, 8(1):78–118, 2005.