# Toward Optimal Multi-Objective Models of the Network Security: Survey

Valentina Viduto(Presenting Author), Wei Huang and Carsten Maple
Institute for Research in Applicable Computing (IRAC)
University of Bedfordshire
Luton, United Kingdom
valentina.viduto@beds.ac.uk, wei.huang@beds.ac.uk and carsten.maple@beds.ac.uk

**Abstract — Information security is an important aspect of a successful business today. However, financial difficulties and budget cuts create a problem of selecting appropriate security measures and keeping networked systems up and running. Economic models proposed in the literature do not address the challenging problem of security countermeasure selection. We have made a classification of security models, which can be used to harden a system in a cost effective manner based on the methodologies used. In addition, we have specified the challenges of the simplified risk assessment approaches used in the economic models and have made recommendations how the challenges can be addressed in order to support decision makers.**

**Keywords-risk assessment; multi-objective models; network security optimisation; visualisation techniques;survey;**

## I. INTRODUCTION

Today's IT infrastructures, systems and applications are more integrated, dynamic and distributed. According to [1] we have reached the era where information is the key for business to thrive and never before, information has been so important. With the rapid development of Information Technologies (IT) and increased popularity to run business online, networked systems are becoming increasingly vulnerable to cyber attacks. As a result, attacks can influence the productivity, revenue and reputation. Thus, there is a need to know the possible chances of securing informational assets in the environment where the number of attacks and threats emerge rapidly [2]. The models developed recently are oriented towards better analysis and assessment of threats, risks, vulnerabilities and network security measures. But even with the presence of such models, security measures cannot always protect assets from threats. This is because of a poor network assessment and inherent management weaknesses. Hence, the security risk can never be fully eliminated, because it cannot be predicted. Though, the security models today should be designed to help security administrators and decision makers to take effective decisions when a number of constraints is considered.

Network risk assessment plays a crucial role in modern society and is one of the important processes of information security management. A risk management process is needed in order to identify, describe and analyse network vulnerabilities. The final goal of a standard risk assessment procedure is to make security specialists and managers aware of the possible risks, network state and to help them to adopt security measures effectively. However, to be cost-effective, a coherent, well structured and straight forward risk assessment procedure should include the relationships among vulnerabilities, threats and countermeasures. The common methodologies are ISO 27001, ISO 17799 and guidelines issues by the National Institute of Standards and Technology NIST SP800-30 [3, 4, 5].

Usually two approaches can be used to assess systems for risks. One of them is a qualitative risk assessment approach. It uses modelling, visualization techniques to give an overview of the state a system holds, whilst quantitative approach tries to give a measure for risk. In recent literature, researches argue, that combining both approaches can be more beneficial than using these approaches separately [6].

With the high increase of automated systems and tools, humans have gained an ability to visualise, design and model networked systems, their security states, connection paths and other security related factors. Modelling techniques have been receiving a great interest between researchers. In terms of modelling, attack trees, attack graphs and other visualization techniques, such as onion skin model, offer a goal-oriented perspective of multi-stage attacks, help to estimate with the attack related costs, visualize dependencies between vulnerabilities and security measures [6, 7, 8, 9, 10 ]. Despite the advantages modelling techniques offer, they cannot be used for very large networks. The graphs are complex and hard to read.

This paper investigates security models, which consider risk assessment approaches to be applied for threat modelling, network hardening and risk analysis. Furthermore, we discuss the challenges related with the cost effective selection of countermeasures as well as clearly define research gaps in the area of risk assessment.

The remainder of the paper is organised as follows. In Section II, we present visualisation techniques, which often are applied for quantitative and qualitative risk assessment approach. In Section III we discuss security models, which apply risk assessment based methodologies to estimate risk. Section IV provides main challenges and

limitations. In Section V we illustrate our research model which is used to address limitations in the field. Finally we conclude in Section VI.

## II. INCREASING NETWORK SECURITY BY APPLYING VISUALISATION TECHNIQUES

### A. Visualisation Techniques

In order to identify and assess informational assets for threats, vulnerabilities and risks, and implement risk management practices to counteract them, it is necessary to have a clear picture of a state the network holds. Further to this, every security specialist can analyse the prospective adversaries and propose related security measures. With the complete picture, the risk and cost effective strategies can be used to make decisions, based not only on the expertise of the security specialist, but also based on data obtained through particular scenarios and examples [29].

Visualisation techniques can help to convert abstract data so that it can be more informative and easier to understand. The semantic analysis of information gathered from abstract data should provide knowledge that will support decision-makers in finding a solution on how systems should be protected. Being more practical, a graph which interconnects various aspects in a compact way is worth more than a long explanation.

In general, visualisation techniques are widely applied to analyse network security level and predict attacks, risks and possible threats. These techniques are attack graphs and attack trees. Attack graphs can represent all potential vulnerabilities and potential attack paths an attacker can take in order to reach the target. Furthermore attack graphs act as a tool in finding critical paths in large networks based on the threats and vulnerabilities identified. However, initial attack graph for large size networks was complex and visually not clear due to number of attack paths. Later, by enhancing the visualisation of the graph and proposing monotonicity concept, attack graphs became more scalable [30]. As a result, the layout of an attack graph can be adjusted to represent the real enterprise network.

Attack graphs are often applied for network hardening in order to effectively represent a prior knowledge about vulnerabilities, their dependencies and network connectivity. In a graph, each path is an exploit that can have undesirable impact on system (Figure 1a).

Attack trees are often applied for quantitative risk assessment analysis, because of the simplified way of visualising network nodes, attacks and their dependencies. According to [29] the concept of a tree can be used to analyse and assess the attributes of a security system, e.g., a probability of an attack success, assess the risks and quantify the costs of possible damage and defence controls. In terms of quantitative risk assessment, a tree structure can help to quantify lowest cost security countermeasure and the total cost of an attack.

This research is financially supported by EPSRC

For more information about visualisation techniques applied for network hardening, please refer to [10, 25, 29].

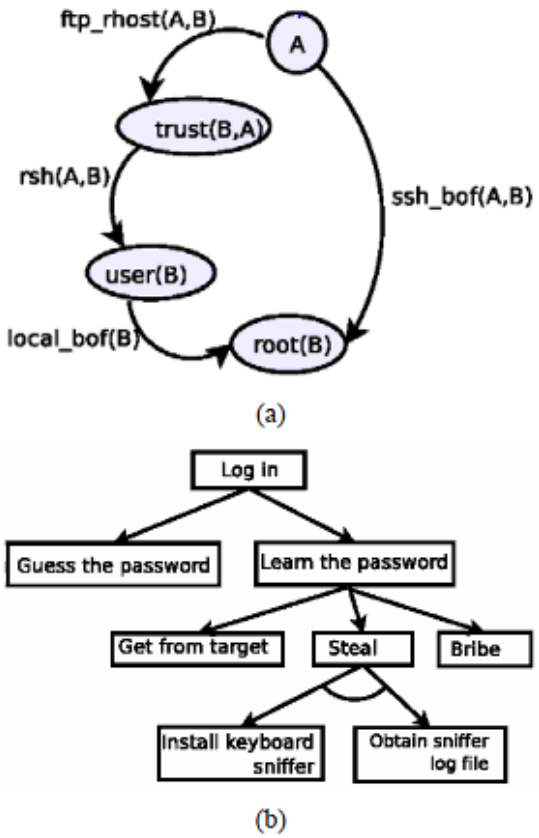


Figure 1. Attack scenarios by applying attack graph (a), attack tree (b)[29].

## III. SECURITY MODELS

Security of information assets is a priority for most organisations today. Investments are made to harden the perimeter, network devices, software bugs and to increase user awareness, however, to distinguish whether the investment was cost effective is a challenging task.

Researchers have developed a number of security models for valuating security investments and optimally investing into information security [11,12]. Differently from these models, the authors in [13, 21] have proposed a model which analyses optimal defence strategy as a finite game between an attacker and defender

In overall, security models can be classified based on the methodologies used to optimally invest into computer security. We have specified the following:

- Risk assessment models
- Cost-benefit models
- Game models
- Multi-objective decision support models

All of these methodologies help to distinguish how much should be invested into computer security, what benefits an organisation would get from certain investment and optimal allocated resources, so an attacker would not have adverse effect on informational assets.

### A. Risk Assessment Models

First, risk assessment is one of the risk management procedures, which mainly provide guidelines in order to identify vulnerabilities, threats and their dependencies. The final goal of the process is to let decision makers be aware of possible risks that should be reduced, transferred or taken.

In general, risk assessment can be undertaken in two ways, by applying qualitative or/and quantitative analysis methods. Qualitative methods require a good knowledge in the areas of vulnerability assessment, threat analysis to correctly predict probabilities of various attacks and possible impacts on the assets [22]. Quantitative approaches offer mathematical methods for calculating risks, impacts and other relative cost factors.

We have made a comparison of risk assessment models analysed in the literature to help evaluate IT security investments. Table I summarises the main characteristics of the methodologies which can be used to calculate Return on Investment (ROI), Return on Attack (ROA) or to estimate the risk value, based on the input data, i.e. value of assets, threat likelihood, vulnerability severity.

The risk assessment models that result in lists of risks, ROI value or set of scenarios do not provide enough information to prioritize risks when multiple resource constraints are considered, e.g. budget or time constraints.

Another drawback of the simplistic risk assessment models relates to their non applicability to the realistic case scenarios. Assessing risks of information security is a very difficult step, because the data on the likelihood and costs associated with the risk factors is often limited and constantly changing. Thus, multi-objective conditions should be considered within the quantitative risk assessment process to optimally invest into network security.

### B. Game Models

Differently from the models covered above, authors in [13][21] have proposed a game-theoretic method for optimal network hardening, where the overall cost for a defender is reduced based on the algorithm proposed. Game theoretical analysis is useful for decision, modelling and control processes related to network security.

An interaction between an attacker and a defender treated as a two-player stochastic game in which action sets, costs/reward functions and transition probabilities can be defined. By creating specific scenarios, a game theory provides information such as attacker's goal, steps he or she will follow, what are the rewards for each of the players, what are the expenses or how are the resources utilised during an attack [25]. Furthermore, game-models can help to estimate optimal network hardening strategies used to defend the attack in advance.

The main drawback of such theory lies in hypothetical assumptions, which may not be applicable in a real state of affairs. The steps an attacker may take are only predictable, so the final resource allocation methodology for a defender may be misleading.

TABLE I. COMPARISON OF RISK ASSESSMENT MODELS

| References | Risk Assessment Models | | |
|---|---|---|---|
| | **Method** | **Input** | **Output** |
| [23] | Quantitative | Threats, Success/Failure data, Asset value | Rik-vulnerability mapping, Risk index |
| [15] | Quantitative | Assets, Threats, Probabilities | ALE, Risk value, Total Damage |
| [2] | Hidden Markov method (HMM) | IDS alerts | Threat index Risk index |
| [7] | Quantitative | Asset values, Actual Threats, Potential Threats, Vulnerabilities, Frequency of threats | Total Risk, Risk for host index |
| [8] | Quantitative | Asset value, Relative ranking of vulnerabilities and threats Exposure factor (EF) ALE, ARO, SLE, Safeguard cost | Return on Investment (ROI) |
| [6] | Qualitative and Quantitative | An attack tree, SLE, ARO, ALE, EF, Safeguard cost, Cost of loss | ROI, Return on Attack(ROA) |
| [24] | Quantitative and Qualitative | Asset value, Severity of Vulnerability, Likelihood of an Attack, SLE, ALE, ARO Attack tree | ROI |

### C. Economic Models with the Cost-benefit Analysis

Cost-benefit analysis looks into intangible costs/returns and addresses time perspective. The simplicity of the frameworks can give suitable investment solutions for low risk investments. However, these methods do not consider uncertainty and give misleading indications for long term investments.

Arora et.al has proposed a risk management framework, which determines costs and benefits of information security solutions [14]. They evaluate investments based on the benefits each invested dollar of investment brings, as well as reduce expected loss or risk.

Furthermore, a cost-benefit trade-off is identified in relation to risk based return on investment (RROI) rather than ROI. To calculate RROI, an incident risk is calculated first (Eq.1). To distinguish between how cost effective the security solution is and how it will affect the incident risk, authors have introduced a bypass rate, which is estimated based on the effectiveness of it to an incident type.

$$IncidentRisk = \frac{\text{Observed damage (incident type)}}{Net \text{ bypass rate (incident type)}} \quad (1)$$

The model is rather hypothetical than practical because of the challenges in estimating bypass rate of the security solution and obtaining true costs of lost productivity or other possible attack consequences.

The cost-benefit analysis methodology proposed by Wei et.al can be used to calculate the cost of detecting an intrusion and responding to it based on qualitative and quantitative risk management approaches. The overall goal of the methodology is to determine the trade-off between costs required to respond to the IDS events and benefits the investment brings. To calculate the total cost for the event the equation is as follows.

$$\text{Cost\_total} = \text{Progress x DamageCost} + \text{ResponseCost} + \text{OperationCost} \quad (2)$$

From their model, a cost benefit trade-off is calculated and if the response cost is higher than the damage cost, IDS will not log an event; however, in case the response cost is lower than the damage cost, a response to an attack will be initiated. The model is not designed for real time intrusion detection and cost calculation is not effective for this case, however, this model can be used as a background for future developments.

D. Multi-objective Decision Support Models

Best security practice dictates that security requirements be based on risk assessment [17]. However, simplistic risk assessment that as a result lists risks based on the set of pre-defined scenarios do not provide sufficient information. Furthermore, when additional requirements are requested, such as time or budget constraints, these models cannot be applied.

Multi-attribute analysis help decision makers evaluate alternatives when conflicting objectives must be considered and balanced. Once constructed, a multi-attribute analysis framework also provides the basis from which decision makers can evaluate alternative risk-mitigation strategies [17].

The approach to match vulnerabilities to security profiles and enabling organisations to choose a minimal cost security profile providing maximal vulnerability coverage was analysed in [26]. The idea behind their approach is that any given security technology addresses only specific vulnerabilities and could possibly create additional vulnerabilities, named residual vulnerabilities. The authors have made an assumption that if a known vulnerability is covered by a particular security technology, the risk of that vulnerability being exploited is uniform, which most probably in a real case scenario would not always be the truth, as the risk level depends upon the severity of the vulnerability and impact it possesses to a system. The multi-objective problem introduced is to minimise the residual vulnerabilities and cost of implementing security measures. The problem was simplified to a set-covering problem, solved using genetic algorithm (GA) adapted to the weighted sum fitness function (Eq. (3)). As an input, authors have used generic set of security policies capable of covering one or more generic vulnerabilities, previously proposed in [27].

$$F = \alpha \sum_{i=1}^{m} a_i r_i + \beta \sum_{j=1}^{n} c_j s_j \quad (3)$$

Where $\alpha+\beta = 1$ and $\alpha,\beta \leq 1$ represent preferences of the organisation. First objective maximises the coverage of vulnerabilities, or in other words, minimises the weighted residual vulnerability. Second objective minimises the costs to the organisation.

Based on the Butler's initial multi-attribute assessment framework, a multi-objective optimal security hardening problem was formulated in [28]. The authors have modelled the system administrator's decision problem as three optimisation problems on the attack tree model. The transformation of the problems has led to more cost-benefit solutions required by the decision maker. The multi-objective problem then is to find a vector of security measures which minimises the total security control cost and residual damage. To solve problems authors have used SGA and NSGA-II algorithms. From the results obtained by the NSGA-II, only few robust solutions with good balance between residual damage were obtained. The gaps in the Pareto front are signalling that authors have not considered dependencies between the security measures. This limits the ability to provide real life solutions when multiple objectives should be considered.

## IV. CHALLENGES

Based on the state-of-the art work related to risk assessment approaches, when a decision maker has to consider a set of security countermeasures to be applied to increase the security and reduce the risk of possible losses, the main challenge is to combine conflicting factors into an analysis.

From the discussed work, the factors such as cost, risk, threats, likelihood are widely used, however, the issue like how the risk management can help in defining the risk and ways to reduce it, has not been raised before. Currently, there is no particular model introduced in the literature, which would combine general risk

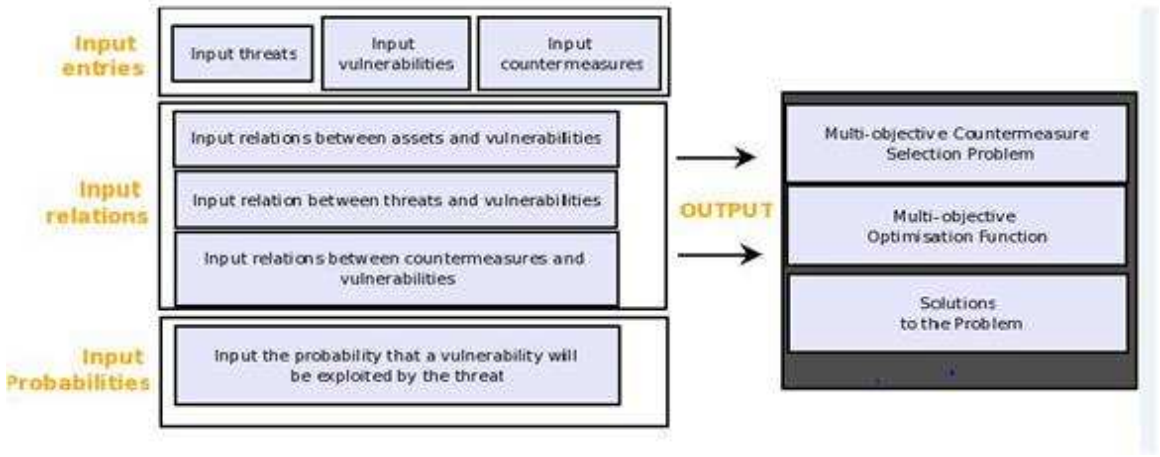


Figure 2. Multi-objective risk assessment model flowchart.

management factors into a multi-objective optimisation problem related to conflicting factors of cost and risk.

Furthermore, in order to be able to answer the question, like "What risk can I accept" simplistic risk assessment models cannot be used. The following criteria should be considered:

- Multiple objectives, which would compound cost related factors.
- Be more practical.
- Consider the impact on confidentiality, integrity, availability (CIA).
- Use of tangible costs.

Considering the factors mentioned above, the model could help in making cost-effective decisions.

## V. Research Recommendations

Based on the challenges covered above, we have designed a model which in a coherent, structured way applies risk assessment procedure and optimisation routine for efficient search of cost effective solutions for multi-objective security countermeasure selection problem.

Figure 2 shows a flowchart of the research model we are working on, where input entries, relations and probabilities are used to formulate a multi-objective countermeasure selection problem and an optimisation function. Applying optimisation techniques, the process of selecting countermeasures can support with cost effective decisions.

## VI. Conclusion

The importance of appropriate security models and risk management procedures in modern society is well understood. There has been an increased interest between the researchers to develop risk based models, which could help in dealing with the identification of threats, vulnerabilities and risks. Despite that, most of the models can only be used to compute effectiveness of investments in terms of calculating the ROI index or are limited by their applicability for real case scenarios.

Visualisation techniques opened an ability to illustrate large data formats so that gained data would be used for knowledge and improved awareness between information system users. Furthermore, use of visualisation techniques helps in identification of threats in networked systems.

## References

[1] C.Maple, P. Phillips, "UK Security Breach Investigations Report", 7Safe, United Kingdom, 2010.

[2] Jie Ma; Zhi-tang Li; Hong-wu Zhang; , "A Fusion Model for Network Threat Identification and Risk Assessment," International Conference on Artificial Intelligence and Computational Intelligence, 2009. AICI '09., vol.1, pp.314-318.

[3] M.Templeman, M. Beishon, L. Malachowski, A.Wilson, T. Nash, L. Robertson, Information security - best practice measures for protecting your business, Tech. rep., Department of Trade and Industry (2005).

[4] ISO/IEC 27001:2005, Information Technology - Security techniques – Information Security Management Systems - Requirements, International Organisation for Standardization (2005).

[5] ISO/IEC 17799:2005, Information technology - Code of practice for information security management (2005).

[6] S. Bistarelli, F. Fioravanti, P. Peretti, "Defense Trees for Economic Evaluations of Security Investment" , *ARES'06*, pp.416-423.

[7] H. Lv, "Research on Network Risk Assessment Based on Attack Probability", International Workshop on Computer Science and Engineering, vol. 2, 2009, pp.376–381.

[8] A. Asosheh, B. Dehmoubed, A. Khani, "A new Quantitative Approach for Information Security Risk Assessment", International Conference on Computer Science and Information Technology 2009, pp. 222–227.

[9] L. Wang, S. Noel, S. Jajodia, "Minimum-cost network hardening using attack graphs", Computer Communications (2006), vol.**29**, pp.3812–3824.

[10] C.Maple, V.Viduto,"A Visualisation Technique for the Identification of Security Threats in Networked Systems", In proceedings of Information Visualisation, 2010, pp.551-556.

[11] T. Bandyopadhyay, "Information Security Investment in Prevention and Detection Regimes – Towards an Aggregate Economic Model," Proceedings of SAIS 2007.pp. 142 – 147.

[12] A. L. Couch, N. Wu, H. Susanto, "Toward a Cost Model for System Administration", Proceedings of the Niteenth Large Installation System Administration Conference (LISA 05),2005, pp. 125-141.

[13] W.Jiang H. Zhang, Z. Tian, X. Song, "A Game Theoretic Method for Decision and Analysis of the Optimal Active Defense Strategy, In Proceedings of the 2007 International Conference on Computational Intelligence and Security (CIS '07), 2007, pp. 819-823.

[14] A.Arora, D. Hall, C. Pinto, D. Ramsey, R. Telang, "Measuring the Risk-based Value of IT Security Solutions", IT Professional vol.6, 2004, pp. 35–42.

[15] A.Ekelhart, S.Fenz, M. Klemen, E. Weippl, "Security Ontologies: Improving Quantitative Risk Analysis, in *"*40th Annual Hawaii International Conference on System Sciences*"*, 2007.

[16] H.Wei, D. Frinke, O. Carter, C. Ritter, "Cost-benefit Analysis for Network Intrusion Detection systems", in *'CSI 28th Annual Computer. Security Conference',* 2001.

[17] S. A. Butler, P. Fischbeck, " Multi-attribute risk assessment", Tech. Report, Proceedings of SREIS01, 2001.

[18] Gupta, M., Rees, J., Chaturvedi, A. & Chi, J. "Matching Information Security Vulnerabilities to Organizational Security Profiles: a Genetic Algorithm Approach", Decision Support Sysemst, vol.41(3), (2006), pp.592–603.

[19] R. Dewri, N. Poolsappasit, I. Ray, D. Whitley, Optimal security hardening using multi-objective optimization on attack tree models of networks, in *'Proceedings of the 14th ACM conference on Computer and communications security',* ACM, 2007 , pp. 204–213.

[20] T.Neubauer, C.Stummer, E.Weippl, "Workshop-based Multi-objective Security Safeguard Selection", International Conference on Availability, Reliability and Security, 2006, pp. 366-373.

[21] W. Jiang, B. Fang, H. Zhang, Z. Tian, X. Song, "Optimal Network Security Strengthening Using Attack-Defense Game Model," Third International Conference on Information Technology: New Generations, , 2009 , pp. 475-480.

[22] G.Y.Liao, C.H.Song, "Design of a Computer-aided System for Risk Assessment on Information Systems", IEEE 37th Annual International Carnahan Conference on Security Technology, 2003, pp. 157-162.

[23] S. Kondakci, "A Composite Network Security Assessment", Proceedings of the Fourth International Conference on Information Assurance and Security, 2008, pp. 249-254.

[24] M. Ketel, "IT security risk management", Proceedings of the 46th Annual Southeast Regional Conference, 2008, pp. 373-376.

[25] V. Viduto, C. Maple, W. Huang, "An Analytical Evaluation of Network Security Modelling Techniques Applied to Manage Threats," International Conference on Broadband, Wireless Computing, Communication and Applications,2010, pp. 117-123.

[26] M. Gupta, J. Rees, A. Chaturvedi, J. Chi, "Matching Information Security Vulnerabilities to Organizational Security Profiles: a Genetic Algorithm Approach', Decis. Support Syst. vol.41(3), 2006, pp. 592–603.

[27] R. H. Anderson, P. M. Feldman, S. Gerwehr, B. Houghton, R Mesic, J. D Pinder, J. Rothenberg, J. Chiesa, "Securing the U.S. Defense Information Infrastructure: A Proposed Approach", Technical report, RAND corporation, 1999.

[28] R. Dewri, N. Poolsappasit, I. Ray, D. Whitley, "Optimal Security Hardening Using Multi-objective Optimization on Attack Tree Models of Networks", in *'CCS '07: Proceedings of the 14th ACM* conference on Computer and communications *security'*, 2007, pp. 204–213.

[29] V. Viduto, C. Maple, W. Huang, "Managing Threats by the Use of Visualisation Techniques*",* Int. J. Space-Based and Situated Computing, Vol. 1, Nos. 2/3, pp. 204–212.

[30] Jha, S., Sheyner, O. and Wing, J. "Two formal analysis of attack graphs", in *CSFW '02:* Proceedings of the 15th IEEE Workshop on Computer Security Foundations, 2002, p. 49.