An analytical evaluation of network security modelling techniques applied to manage threats

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

***Abstract*—The current ubiquity of information coupled with the reliance on such data by businesses, has led to a great deal of resources being deployed to ensure the security of this information. Threats can come from a number of sources and the dangers from those insiders closest to the source have increased significantly recently. This paper focuses on techniques used to identify and manage threats as well as the measures that every organisation should consider to put into action. A novel game-based onion skin model has been proposed, combining techniques used in theory-based and hardware-based hardening strategies.**

Keywords - Attack graph, attack tree, network hardening, threats

I. Introduction

The proliferation of electronic systems and ubiquity of access to the information they hold, increased a risk that a confidential data can be lost or accessed by those criminally minded. In the last few years a number of cases when a confidential data was being compromised has increased. Statistics from Verizon and Ponemon studies on the cost of a data breach showed, that in 2009 a total cost of data breaches continues to increase reaching $202 (US) per compromised record [1], [2]. The statistic is discouraging and the cost of each security incident is extremely high. Despite regulations, laws and awareness of the need to protect information assets, data breaches continue to grow and evolve. From the same statistic source [1], [2], an attack difficulty recorded in 2009 has increased by a few points comparing to the cases recorded in 2008. While ten years ago cybercrime was for a reason of vandalism, now the large increase is for financial gain. On the whole , while the criminals are not working hard in order to compromise the network, decision makers struggling with the implementation of new, more effective systems that would minimise an impact of an incident, if such was.

High demand in development of novel network security strategies and models is highly discussed between researchers and developers. The more the technology evolves the harder it becomes to stabilise the system due to interdependence of the assets and other measures.

This research is financially supported by UK EPSRC, whose support is much appreciated.

A large body of work has been undertaken in the field of network security. However, our analysis concentrates on the models and strategies that have been proposed in order to help decision makers to optimally invest into security safeguards and maximally defend their systems. Furthermore, we pay an attention on the techniques that concentrate on managing internal and external threats. In particular, we are making an analytical evaluation of the network hardening models proposed to identify and manage threats for the purpose of further developments and refinements.

This paper gives an overview of existing models and strategies that have been proposed based on the theoretical and practical analyses, experiments and knowledge. The overview will start from hardening models were attack graphs and attack trees is a common term being used. Followed by identifying the graphs and the trees usefulness, an evaluation will be performed.

An analysis and evaluation of the cost models will concentrate upon the metrics, used to define an optimal strategy and methods to derive a solution.

The remainder of the paper is organised as follows. A background regarding network hardening using modelling techniques is introduced in Section II. A notion of modelling techniques such as attack graphs and attack trees is explained in Section III, as well as the areas of use and appropriateness. In Section IV, we make an analytical comparison of three hardening models, based on the modelling technique, aim, variables used and advantages it provides. In Section V we have proposed an onion skin model based, in particular, on the game-based models. Finally, conclusion is drawn in Section VI.

II. Background

Network hardening is a process or a procedure that is based on vast range of techniques, strategies and methodologies which are used to evade multiple attacks or threats. Hardening a network does not always mean spending large quantities of money. Nevertheless, money are required in some form, whether the hardening procedure is undertaken on changing a hardware or on man power. In fact, hardening procedure depends on what are the needs of each organisatusingion and what has to be addressed. In this sense, the time as a form

of money may come when extra man hours are required to repair the damage revealed due to an exploit.

From the work undertaken on network hardening models, most common modelling techniques used to derive a solution for network hardening is by the use of attack graphs [3], [4], [5] or attack trees [6]. Furthermore, network hardening rarely is used in the theory of game-based models [7], where the game is played between a defender and an attacker in order to effectively analyse each player's strengths and weaknesses. A process of identifying and managing threats is the key destiny of security specialists, in order to effectively run the business and keep the system up and running. In particular, when we talk about computer security, we mean that we are addressing aspects of:

Confidentiality - ensures that computer-related assets can only be accessed by authorised parties

Integrity - means that assets can be modified only by authorised parties and only in authorised ways

Availability - means assets are accessible to authorised parties at appropriate times.

Most of the hardening techniques are addressed to detect external attacks and preventive measures to minimise the damage. However, many organisations are more suffering from insiders than external attackers. This is due to insiders have some level of privileges assigned and some kind of knowledge about preventive measures that they first will try to overcome. Being aware of inside threats, organisations should maximally limit access to the information by implementing strong access control system and other prevention measures. In fact, some level of risk will still remain.

III. Preliminaries

A. A notion of an attack graph

Attack graphs are widely applied in a network hardening concept in order to effectively represent a prior knowledge about vulnerabilities, their dependencies and network connectivity [5]. Each path in an attack graph is a series of exploits, which lead to an undesirable state. The state is an event that has an undesirable impact on the system. Furthermore, such a concept of attack graphs is used to answer questions like "To what attacks is my system vulnerable to?", "How many different ways an attacker can take to reach his goal?", "Which set of measures should an administrator deploy to ensure the attacker cannot achieve his goal?".

According to [8] attack graphs can serve as accompanying tool in several areas of network security, including intrusion detection (in particular help in IDS alert prioritisation) [9], defence, forensic analysis and security policy considerations. There are three different representations for an attack graph. First, an attack graph can accurately enumerate all possible vulnerability sequences (attack paths) an attacker can follow [10]. Nevertheless, such graphs faced scalability problem, due to explosion in the number of attack paths. Second, a monotonicity assumption has partially overcome a scalability problem by making an assumption stating that an attacker never relinquishes an obtained capability. This assumption helped to derive a graph containing all required information about dependency relationships among vulnerabilities [11]. Third, [12] has overcome a scalability problem by constructing a two-layer attack graphs, which in sense have reduced computation cost and simplified the graph itself. The monotonicity assumption is also applied to generate the graph.

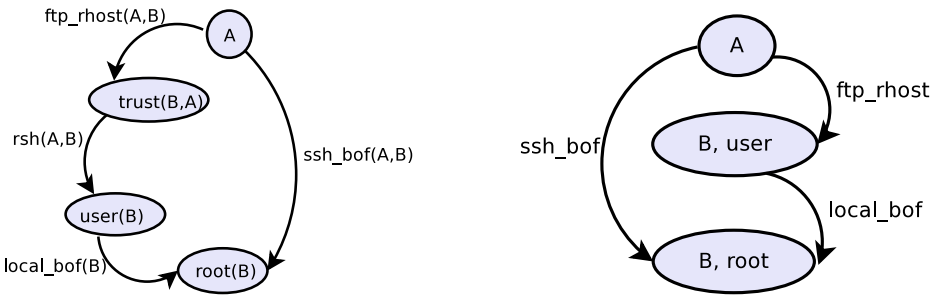
In overall, an attack graph represents all possible attack sequences that an attacker may use to break into a network. An attack sequence is described as a single path in the graph and the dependencies between the paths are the relations between the vulnerabilities. As a result, attack graphs can provide meaningful and quantitative conclusions in analysing network security [12].

Commonly an attack graph can be represented with *exploits* and *conditions* [3]. An exploit is a predicate $v(h_s, h_m, h_d)$, where h_s is a source host from which a vulnerability v was initiated, h_d is a destination host, h_m an intermediate host. However, two hosts can be used as $v(h_s, h_d$, in case of no intermediate hosts exist on the path. A condition is a predicate $c(h_s, h_d)$, where a security condition c is satisfied on source host h_s and destination host h_d (when no intermediate hosts are used). A condition can be treated as an existence of the vulnerability or the connectivity between source and destination hosts. Although, there two types of directed edges that link exploits and conditions. First, an edge that can point from a condition to an exploit denotes the *require* relation. The require relation is always conjunctive and means the exploit cannot be executed unless the condition is satisfied. Second, the edge pointing from an exploit to a condition denotes the *imply* relation, which is always disjunctive. The imply relation means executing the exploit will satisfy the condition [3].

Definition 1 *Given a set of exploits E, a set of conditions C, a require relation $R_r \subseteq CxE$, an imply relation $R_i \subseteq ExC$, an attack graph is $G(E \cup C, R_r \cup R_i)$.*

One important aspect of attack graphs is that an exploit cannot be realised until all conditions have been satisfied. However, some exceptions do exist. In case when an exploit with multiple variations may require different sets of conditions. This case can be handled by having a separate vertex for each variation of the exploit. Another case is when a collection of exploits may jointly imply a single condition. This case is handled by the insertion of dummy conditions to capture the conjunctive relationship [3].

A new approach of two-layer attack graphs has provided an advantage of vividly analysing graphs, finding dangerous hosts inside a network and process several targets at the same time [12]. The generation model consists of *host-pair attack*(Figure 1(b)) and *hosts access* graphs (Figure 1(b)). The host-pair attack graph has the same meaning as an attack graph, where one source host connects to one target host directly. However, the resulting host-pair attack graph is



(a) A host access graph

(b) A host-pair attack graph

Fig. 1. Illustration of attack scenarios by using a host access and host-pair attack graphs.

small in size and is generated quickly. The information used is linked to target host's h_d vulnerabilities, configurations and its network connection to the source host h_s. The hosts access graph shows the number of hosts in the network and the attacker's access privilege transition between hosts. This graph is build based on the host-pair attack graph. A directed edge represents the access relationship between two hosts. In case an attacker can obtain a root privilege on target host h_d the directed edge will be placed between corresponding nodes.

B. A notion of an attack tree

Similarly to attack graphs, attack trees are used to visualise a networked system containing possible risks and attack paths. The structure of the tree is more convenient than in attack graphs, due to simplified categorisation of ways a system can be attacked. The term was first introduced by Schneier [13]. In an attack tree, the nodes represent attacks. The root node in the tree is a destination of the attacker, in other words, is the goal of an attacker. Children of a node are refinements of this goal and leafs represent attacks that can no longer be refined [14]. Moreover, there are AND and OR nodes. OR nodes are alternatives - for example, two ways to get into a building. AND nodes represent different steps in achieving a goal. An attacker cannot achieve the final goal unless both subgoals are satisfied. The tree concepts can be used to analyse attributes of the security of the system, for example, probability of an attack success, the cost, cheapest low-risk attack, defence methods, whether special tools are needed. How does this work? First, the value should be assigned for each node, in fact, nodes will have different values corresponding to many different variables. Second, prioritise the nodes according to the value determined. This will give information on what nodes are more critical and require more attention.
A basic attack tree is shown in Figure 2(a). This graph helps to identify possible risks, such as eavesdropping or dictionary attack, that could be avoided if appropriate measures would be in place. Such measures are the use of strong passwords, do not share your login details with anyone or stick them in front of the monitor.

Example of a cost analysis by the use of an attack tree is shown in Figure 2(b). This kind of analysis can give information on the cost of an attack. Using quantitative metrics, the value of an attack can be calculated and the further assessment undertaken.

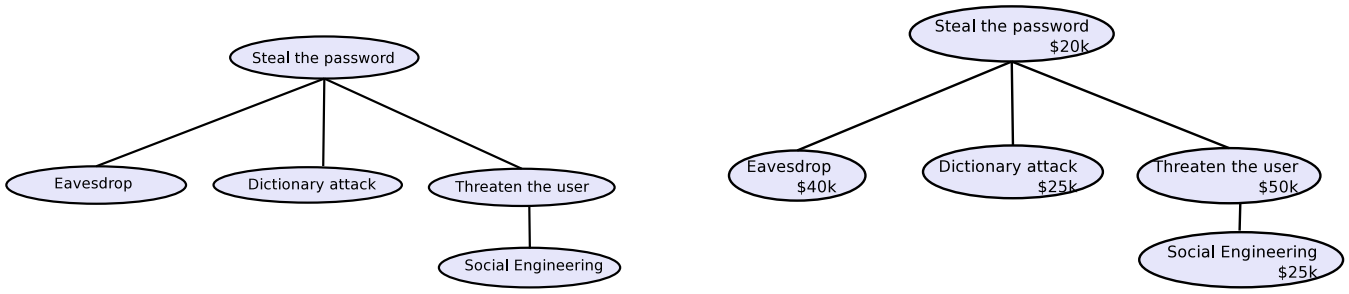
IV. Hardening Models

For the purpose of evaluation we have made a classification of network hardening models based on the methodology used. Each of the models in some way use modelling techniques to identify threats, either internal or external, however, the aim of the hardening models differs.

1) Theory-based models (Risk management, assessment strategies)
2) Game-theory models
3) Hardware based hardening models (IDS/IPS, Firewall)

Theory-based models are the ones that concentrate on the risk assessment process used to assess the likelihood of an event occurring, implement measures that are designed to reduce the risk and ensure that an organisation can respond to an event so that the consequences will be minimised [16]. The common idea used in this type of models is an implementation of risk assessment strategies used to identify and manage threats. Risk assessment process generally can be assessed by implementing qualitative and quantitative metrics and techniques. The qualitative scenarios can be illustrated by modelling attack trees [15], [6] and determining the path in the tree that could lead to disastrous state. This approach is widely used to visualise possible threats. Attack graphs, as a modelling technique is not applicable to assess the likelihood of events occuring, as it is time consuming and error-prone to justify the value of risks and investing into security controls from the complex generated graph. The quantitative approach uses quantitative metrics and help decision makers to select among number of good value security solutions a most profitable one gained from the risk assessment methodology. Use of attack trees for quantitative risk assessment is not effective, because it is difficult, or even impossible, to obtain the actual costs related to an incident and threats, either internal or external, evolve over time.

Game-theoretical analysis is useful for analysing, modelling, decision and control processes for network security [7].



(a) An attack tree

(b) Cost of an attack

Fig. 2. Illustration of an attack tree including a cost of an attack.

TABLE I
COMPARATIVE EVALUATION OF HARDENING MODELS

	Risk Assessment [15]	Attack-Defence Game model [7]	IDS sensor placement [9]
Technique used	Attack trees Defence Trees	Defence graphs Attack graphs	Attack graphs
Aim	Identify threats Determine the value of an attack	Strengthening the system Minimise the cost of an attack	Optimal IDS sensor placement Discover multi-step attacks
Variables	Single Loss Expectancy (SLE) Annual Rate of Occurrence (ARO) Expected gain from attacker Cost of safeguards Costs of an attack	Attack damage Defence operation cost Residual damage Negative damage Defence cost	Host configuration Vulnerable services Network connectivity Critical network assets Threat sources
Advantage	Combination of qualitative and quantitative methods Combination of Return on Security Investment (ROSI) and Return on Attack (ROA)	Total cost of security guards is minimised	An attack graph comprising all known attacks Optimal number of sensors
Disadvantage	Interactions between safeguards are not considered Lack of empirical data for SLE and ARO	Simplistic model Determining input variables is difficult	Alerts are prioritised based on attacks closer to a critical asset Graph is complex

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 a specific scenarios, game theory provide an information such as attacker's goal, steps he or she will follow, what are the reward for each of the players, what are the expenses or how are the resources utilised during an attack. Furthermore, this methodology can be used not just to calculate a total cost of implementing security safeguards, but minimise it and being within budget. However, a game-theoretical analysis is rarely used for managing insider threats.

Hardware based hardening strategies closely relate to intrusion detection/ prevention system (IDS/IPS) and firewall rules and actions [17], [18]. The actions initiated by the IDS are largely discussed in the literature [19], [20]. Optimisation of IDS sensors, optimal placement and minimisation of false positives and false negatives is a prime concern for decision makers. Efficient fitness functions solve the cost problem for triggered false alarms and related responses, thus, increasing better IDS/IPS performance. This type of strategies is mostly oriented on traffic monitoring and anomaly detection and is widely applied for misuse detection.

The three types of proposed hardening strategies are summarised in Table I.

From Table I, attack graphs and attack trees are used as a supplementary modelling technique used to visualise all possible attack paths, vulnerabilities and vulnerability dependencies. The use of modelling techniques help to solve vul-

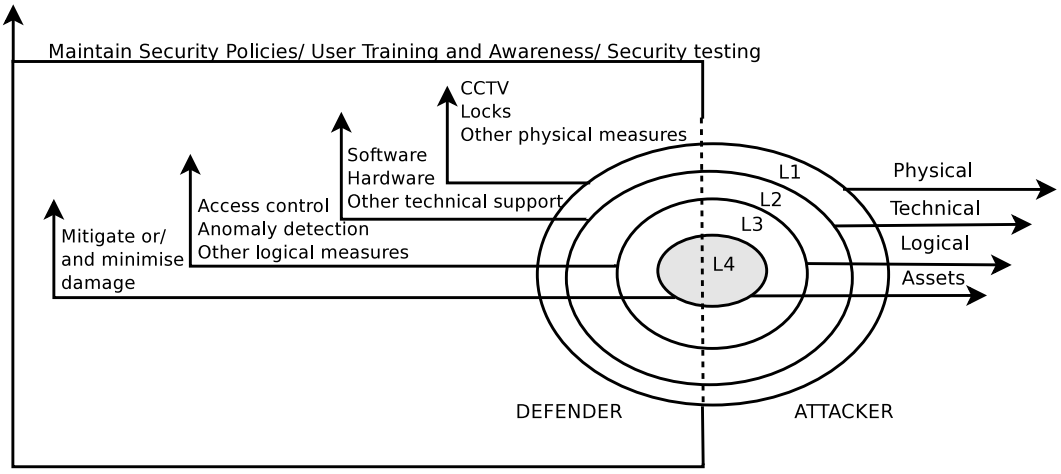


Fig. 3. Generic onion skin model

nerability dependencies, predict possible attacks and estimate the cost for known measures.

The risk assessment strategy proposed in [15] combines qualitative and quantitative methods to evaluate effectiveness and economic profitability of countermeasures as well as their deterrent effect on attackers. Use of attack trees as well as defence trees gives a concept of how threats could be managed and dealt with. An economic analysis using quantitative metrics assigned to assumed attacks extends the method of managing costs as well as security of the system. However, the model is not time based and the risk assessment performed yesterday might have very different results if performed tomorrow.

Hardware based models, in particular, where IDS/IPS, firewalls are used to monitor the traffic either network or host, to detect any anomaly, unknown patterns effectively can be applied to manage insider threats as well as external ones. The attack graphs are more applicable for this type of models as they help to enumerate possible vulnerabilities,comprise possible insider threats, optimise number of sensors and minimise the control costs.

The game-theory is rarely used in relation to attack modelling techniques and insider threat management. However, the outcome of the common mathematical functions formally construct the possible actions of each player. Hardware based strategies generally concentrate on IDS/IPS functionality, traffic monitoring and optimisation of number of sensors and their placement. Optimised number of sensors and maximised efficiency of traffic monitoring help to detect an attack and initialise an appropriate prevention action.

V. Insider threats and hardening measures

Paradoxically, despite of the prevalence of the continuous user training and increased awareness of security threats, the concern of the cases of fraud, espionage or sabotage is raising among organisations due to attacks are approached by those who know the system best: the insiders. Insider threats are particularly devastating as all insiders are granted some level of privilege and trust. At most organisations more effort are putting against the external threats than the internal ones. Why? The reason is simple: it is easier to stop, predict and control. To predict insider activities requires much administrative effort which, in fact, is concentrated on monitoring external sources.

A. Analysis of insider threats and proposed model

Insider threats are the most difficult traceable and predictable threats due to insufficient access controls, policy management, accidental or intentional data leakage and other activities that can violate confidentiality and integrity. Statistics show, that in many cases data was compromised as a result of stolen or lost laptops, USB flash drives or other hardware adopted for data storage [2]. The activities such as social engineering, phishing scams, sabotage, theft of intellectual property, employee fraud are the ones that always keep the company at risk and hardly can be controlled.

One is saying: ”Prevention of an attack is ideal, but detection is a must”. In fact, organisations always try to prevent attacks as much as possible, however, the problem with insider threat is that prevention does not scale very well. If someone is intended to steal a piece of data he is going to do so. Therefore, preventive measures should be teamed with detective measures. Insiders usually have some knowledge about network architecture and first will work around the prevention measures. In this case, all actions should be put to control and detect this activity in order to take follow-up actions to stop insiders by prosecuting or taking other measures against them [21].

Definition 2 *The insider threat is one or more individuals with the access and/or knowledge of organisation or enterprise that would allow to exploit existing vulnerabilities in network security, systems and services with the intent to cause harm or financially benefit from malicious act.*

The generic game-theory model using onion skin notation

is shown in Figure 3. We have categorised insider's step-by-step activity as four level procedure, that in some ways should be achieved. A level one, is a physical access to the system. An insider can overcome this layer by pretending to be an authorised person, social engineering attack or other methods that can be helpful in achieving the target. A level two, is a technical layer, where all technical knowledge about organisational architecture will be used in order to act undetected. A level three is a logical layer, where all authentication/authorisation, access control systems reside. The fourth level is the most critical as the data that can be copromised, altered or sold resides here. From the Figure 3, we call this level as assets. We assume that assests are servers or data stored on databases. Furthermore, we assume that it is not always a must to follow a step-by-step process. The final goal of exploiting a database or stealing it manually can be successfully achieved by jumping over the levels or starting from a particular one.

On the left side of the onion model in Figure 3, a security measures are deployed by defender. Each level in attackers procedure can be controlled either by having CCTV installed on site or by using strong access control systems. All hardening measures that the defender will implement in some way will stop or delay insider's attempts. Major concepts and issues that a defender should implement and maintain are:

- Maintain a vulnerability management program
- Risk and threat categorisation and assessment
- Insider computer fraud anomaly detection
- Information security pattern analysis
- Access control measures, track and monitor all access to network resources
- Security awareness program
- Maintain a security policy
- Security testing

VI. Conclusions

The importance of appropriate security and risk management in modern society is well understood. However, there are a number of methods available to security practitioners to assist them in their decision making. In this paper we have presented an analytical comparison of models where modelling techniques such as attack graphs and attack trees are used for detecting vulnerabilities, visualising their dependencies and estimating the cost of possible attacks as well as finding a minimal cost hardening measure.
Furthermore, we have proposed an onion skin model as a modelling technique for managing insider threats. This model is game-theory based and includes the defensive measures that are vital in hardware/software and theory - based models, such as the implementation of IDS/IPS, firewalls, risk management and assessment. The model can be used to estimate a cost of each defensive measure as well as cost of attack on each onion skin level.

References

[1] Ponemon, "Fourth annual US cost of data breach study," 2009.
[2] Verizon, "2009 data breach investigations report," 2009.
[3] L. Wang, S. Noel, and S. Jajodia, "Minimum-cost network hardening using attack graphs," *Computer Communications*, vol. 29, no. 18, pp. 3812–3824, 2006.
[4] S. Noel, S. Jajodia, B. O'Berry, and M. Jacobs, "Efficient minimum-cost network hardening via exploit dependency graphs," in *ACSAC*, 2003, pp. 86–95.
[5] F. Chen, L. Wang, and J. Su, "An efficient approach to minimum-cost network hardening using attack graphs," in *IAS*, 2008, pp. 209–212.
[6] R. Dewri, N. Poolsappasit, I. Ray, and D. Whitley, "Optimal security hardening using multi-objective optimization on attack tree models of networks," in *ACM Conference on Computer and Communications Security*, 2007, pp. 204–213.
[7] W. Jiang, H. Zhang, Z. Tian, and X. fang Song, "A game theoretic method for decision and analysis of the optimal active defense strategy," in *CIS*, 2007, pp. 819–823.
[8] O. M. Sheyner, "Scenario graphs and attack graphs," Ph.D. dissertation, Pittsburgh, PA, USA, 2004, chair-Wing, Jeannette.
[9] S. Noel and S. Jajodia, "Optimal ids sensor placement and alert prioritization using attack graphs," *J. Network Syst. Manage.*, vol. 16, no. 3, pp. 259–275, 2008.
[10] S. Jha, O. Sheyner, and J. M. Wing, "Two formal analys s of attack graphs," in *CSFW*, 2002, pp. 49–63.
[11] P. Ammann, D. Wijesekera, and S. Kaushik, "Scalable, graph-based network vulnerability analysis," in *ACM Conference on Computer and Communications Security*, 2002, pp. 217–224.
[12] A. Xie, Z. Cai, C. Tang, J. bin Hu, and Z. Chen, "Evaluating network security with two-layer attack graphs," in *ACSAC*, 2009, pp. 127–136.
[13] B. Schneier, "Attack trees: Modeling security threats," *Dr. Dobb's Journal*, vol. 24, no. 12, pp. 21–29, 1999.
[14] S. Mauw and M. Oostdijk, "Foundations of attack trees," in *ICISC*, 2005, pp. 186–198.
[15] S. Bistarelli, F. Fioravanti, and P. Peretti, "Defense trees for economic evaluation of security investments," in *ARES*, 2006, pp. 416–423.
[16] L. A. Gordon and M. P. Loeb, "The economics of information security investment," *ACM Trans. Inf. Syst. Secur.*, vol. 5, no. 4, pp. 438–457, 2002.
[17] S. Acharya, J. Wang, Z. Ge, T. Znati, and A. Greenberg, "Simulation study of firewalls to aid improved performance," in *ANSS '06: Proceedings of the 39th annual Symposium on Simulation*. Washington, DC, USA: IEEE Computer Society, 2006, pp. 18–26.
[18] H. Salehi, H. Shirazi, and R. A. Moghadam, "Increasing overall network security by integrating signature-based nids with packet filtering firewall," in *JCAI*, 2009, pp. 357–362.
[19] H. Nguyen, K. Franke, and S. Petrovic, "Improving effectiveness of intrusion detection by correlation feature selection," in *ARES*, 2010, pp. 17–24.
[20] J. B. Alís, A. Orfila, and A. Ribagorda, "Improving network intrusion detection by means of domain-aware genetic programming," in *ARES*, 2010, pp. 327–332.
[21] E. Cole and S. Ring, *Insider Threat: Protecting the Enterprise from Sabotage, Spying, and Theft*. Syngress Press, 2006.