[1] E. Al-Shaer, H. Hamed, R. Boutaba, and M. Hasan. Conflict classification and analysis of distributed firewall policies. *IEEE Journal on Selected Areas in Communications*, 23(10):2069-2084, October 2005. [bib | DOI | .pdf]

Firewalls are core elements in network security. However, managing firewall rules, particularly, in multifirewall enterprise networks, has become a complex and error-prone task. Firewall filtering rules have to be written, ordered, and distributed carefully in order to avoid firewall policy anomalies that might cause network vulnerability. Therefore, inserting or modifying filtering rules in any firewall requires thorough intrafirewall and interfirewall analysis to determine the proper rule placement and ordering in the firewalls. In this paper, we identify all anomalies that could exist in a single- or multifirewall environment. We also present a set of techniques and algorithms to automatically discover policy anomalies in centralized and distributed firewalls. These techniques are implemented in a software tool called the "Firewall Policy Advisor" that simplifies the management of filtering rules and maintains the security of next-generation firewalls.

[2] T. Alpcan and T. Basar. A game theoretic analysis of intrusion detection in access control systems. In *Proceedings of the 43rd IEEE Conference on Decision and Control (CDC)*, volume 2, pages 1568-1573, December 2004. [bib]

We present a game-theoretic analysis of intrusion detection in access control systems. A security game between the attacker and the intrusion detection system is investigated both in finite and continuous-kernel versions, where in the latter case players are associated with specific cost functions. The distributed virtual sensor network based on software agents with imperfect detection capabilities is also captured within the model introduced. This model is then extended to take the dynamic characteristics of the sensor network into account. Properties of the resulting dynamic system and repeated games between the players are discussed both analytically and numerically.

[3] S. A. Butler and M. Shaw. Incorporating nontechnical attributes in multi-attribute analysis for security. In *Proceedings of the 4th Workshop on Economics-Driven Software Engineering Research (EDSER*, May 2002. [bib]

[4] P. Eronen and J. Zitting. An expert system for analyzing firewall rules. In *Proceedings of the 6th Nordic Workshop on Secure IT Systems (NordSec)*, pages 100-107, Copenhagen, Denmark, November 2001. [bib | .pdf]

[5] D. Frincke. Balancing cooperation and risk in intrusion detection. *ACM Transactions on Information and System Security*, 3(1):1-29, 2000. [bib | DOI]

Early systems for networked intrusion detection (or, more generally, intrusion or misuse management) required either a centralized architecture or a centralized decision-making point, even when the data gathering was distributed. More recently, researchers have developed far more decentralized intrusion detection systems using a variety of techniques. Such systems often rely upon data sharing between sites which do not have a common administrator and therefore cooperation will be required in order to detect and respond to security incidents. It has therefore become important to address cooperation and data sharing in a formal manner. In this paper, we discuss the detection of distributed attacks across cooperating enterprises. We begin by defining relationships between cooperative hosts, then use the take-grant model to identify both when a host could identify a widespread attack and when that host is at increased risk due to data sharing. We further refine our definition of potential identification using access, integrity, and cooperation policies which limit sharing. Finally, we include a brief description of both a simple Prolog model encorporating data sharing policies and a prototype cooperative intrusion detection system.

[6] A. Fuchsberger. Intrusion detection systems and intrusion prevention systems. *Information Security Technical Report*, 10(3):134-139, 2005. [bib | DOI]

[7] C. Iheagwara, A. Blyth, T. Kevin, and D. Kinn. Cost effective management frameworks: the impact of IDS deployment technique on threat mitigation. *Information & Software Technology*, 46(10):651-664, 2004. [bib | DOI]

In this paper we measure the financial benefit of an intrusion detection system (IDS) deployment. To

this end, we use a standard risk analysis framework and extend it by introducing the Cascading Threat Multiplier (CTM). The idea behind the CTM is that a security compromise incurs two types of costs: (a) The direct cost of lost integrity/confidentiality/availability, and (b) the indirect cost, of the compromised component serving as a potential stepping stone for future attacks. The CTM tries to capture the second type of costs, which are typically ignored in the classic risk analysis framework. We propose new risk analysis formulas that tie the CTM concept into accurate calculation of Return on Investment (ROI), otherwise commonly known as Return on Security Investment. Finally, through a case study we demonstrate the effect of IDS deployment techniques on threat mitigation and the ROI. The result of the case can be used to support effective decision-making about which techniques are appropriate for the cost effective management of the IDS in a given environment.

[8] W. Lee, W. Fan, M. Miller, S. Stolfo, and E. Zadok. Toward cost-sensitive modeling for intrusion detection and response. *Journal of Computer Security*, 10(1/2):5-22, 2002. [bib | http]

Intrusion detection systems (IDSs) must maximize the realization of security goals while minimizing costs. In this paper, we study the problem of building cost-sensitive intrusion detection models. We examine the major cost factors associated with an IDS, which include development cost, operational cost, damage cost due to successful intrusions, and the cost of manual and automated response to intrusions. These cost factors can be qualified according to a defined attack taxonomy and site-specific security policies and priorities. We define cost models to formulate the total expected cost of an IDS, and present cost-sensitive machine learning techniques that can produce detection models that are optimized for user-defined cost metrics. Empirical experiments show that our cost-sensitive modeling and deployment techniques are effective in reducing the overall cost of intrusion detection.

[9] M. Papadaki and S. Furnell. IDS or IPS: what is best? *Network Security*, 2004(7):15-19, July 2004. [bib | DOI]

Intrusion detection systems (IDS) have become one of the most common countermeasures in the network security arsenal. But while other technologies such as firewalls and anti-virus provide proactive protection, most current IDSs are passive; detection of a suspected intrusion typically triggers a manual response from a system administrator. Too often, this comes too late.

[10] T. S. Sobh. Wired and wireless intrusion detection system: Classifications, good characteristics and state-of-the-art. *Computer Standards & Interfaces*, 2005. In press, corrected proof, available online 26 August 2005. [bib | DOI]

In computer and network security, standard approaches to intrusion detection and response attempt to detect and prevent individual attacks. Intrusion Detection System (IDS) and intrusion prevention systems (IPS) are real-time software for risk assessment by monitoring for suspicious activity at the network and system layer. Software scanner allows network administrator to audit the network for vulnerabilities and thus securing potential holes before attackers take advantage of them.

In this paper we try to define the intruder, types of intruders, detection behaviors, detection approaches and detection techniques. This paper presents a structural approach to the IDS by introducing a classification of IDS. It presents important features, advantages and disadvantages of each detection approach and the corresponding detection techniques. Furthermore, this paper introduces the wireless intrusion protection systems.

The goal of this paper is to place some characteristics of good IDS and examine the positioning of intrusion prevention as part of an overall layered security strategy and a review of evaluation criteria for identifying and selecting IDS and IPS. With this, we hope to introduce a good characteristic in order to improve the capabilities for early detection of distributed attacks in the preliminary phases against infrastructure and take a full spectrum of manual and automatic response actions against the source of attacks.

[11] J. W. Ulvila and J. John E. Gaffney. Evaluation of intrusion detection systems. *Journal of Research of the National Institute of Standards and Technology*, 108(6):453-473, November-December 2003. [bib | .pdf]

This paper presents a comprehensive method for evaluating intrusion detection systems (IDSs). It

integrates and extends ROC (receiver operating characteristic) and cost analysis methods to provide an expected cost metric. Results are given for determining the optimal operation of an IDS based on this expected cost metric. Results are given for the operation of a single IDS and for a combination of two IDSs. The method is illustrated for: 1) determining the best operating point for a single and double IDS based on the costs of mistakes and the hostility of the operating environment as represented in the prior probability of intrusion and 2) evaluating single and double IDSs on the basis of expected cost. A method is also described for representing a compound IDS as an equivalent single IDS. Results are presented from the point of view of a system administrator, but they apply equally to designers of IDSs.

[12] J. Yu, Y. V. R. Reddy, S. Selliah, S. Kankanahalli, S. Reddy, and V. Bharadwaj. TRINETR: An intrusion detection alert management system. In *Proceedings of the 13th IEEE International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises (WETICE)*, pages 235-240, Washington, DC, USA, 2004. IEEE Computer Society. [bib | DOI]

In response to the daunting threats of cyber attacks, a promising approach is computer and network forensics. Intrusion Detection System is an indispensable part of computer and network forensics. It is deployed to monitor network and host activities including data flows and information accesses etc. But current intrusion detection products presents many flaws including alert flooding, too many false alerts and isolated alerts etc. This paper describes an ongoing project to develop an intrusion alert management system-TRINETR. We present a collaborative architecture design for multiple intrusion detection systems to work together to detect real-time network intrusions. The architecture is composed of three parts: Alert Aggregation, Knowledge-based Alert Evaluation and Alert Correlation. The architecture is aimed at reducing the alert overload by aggregating alerts from multiple sensors to generate condensed views, reducing false positives by integrating network and host system information into alert evaluation process and correlating events based on logical relations to generate global and synthesized alert report. The first two parts of the architecture have been implemented and the implementation results are presented in this paper.

[13] M. Zaki and T. S. Sobh. A cooperative agent-based model for active security systems. *Journal of Network and Computer Applications*, 27(4):201-220, November 2004. [bib | DOI]

This paper presents a multi-agent model for implementing active security concepts. In this model, a group of agents can carry out their tasks cooperatively in order to achieve an ultimate security goal. Thus a low-level module of the proposed model reads the values of interesting data items of the relevant current network events and passes them to a relational database. Comparing these measurements against predefined values in an intruder signature database may point to a particular attack.

The proposed model consists of two parts. (1) A multiagent Intrusion Detection System (MIDS) for detecting attacks. (2) An Active Security Mechanism (ASM) for taking active, network-wide, response against attackers. The proposed approach provides a customizable host environment built from various systems software components to allow an optimal match between the intrusion circumstances and the underlying security architecture. Thus, different frameworks can support alternative responses of existing security services. In addition, the ASM can take rapid response against attacks by making use of sensible sharing of attack intelligence. System agents communicate with each other on different hosts using an agent communication language through a message router.
