Journal of Computer Science 3 (7): 478-486, 2007
ISSN 1549-3636

[1]Roman V. Yampolskiy and [2]Venu Govindaraju
[2]Center for Unified Biometrics and Sensors and Department of Computer Science and Engineering and [1]IGERT in GIS
University at Buffalo, Buffalo, NY 14260, USA

Abstract: In this work we have reviewed studies which survey all aspects of computer security including attackers and attacks, software bugs and viruses as well as different intrusion detection systems and ways to evaluate such systems. The aim was to develop a survey of security related issues which would provide adequate information and advice to newcomers to the field as well as a good reference guide for security professionals.

Keywords: Attacker, IDS, Taxonomy, Software flaw, Virus

INTRODUCTION

As computer systems become more and more important to our every day lives it is necessary to protect them from actions that attempt to compromise the reliability, confidentiality or availability of such systems[1, 2]. In the context of information systems, intrusion refers to any unauthorized access, not permitted attempt to access or damage, or malicious use of information resources[3, 4]. Intrusion Detection (ID) is defined as detection of break-ins and break-in attempts via automated software system[5].

Intrusion detection systems can be grouped into two large categories: knowledge-based or behavior-based[6-9]. Majority of currently deployed systems are knowledge-based, matching signatures of well-known attacks against state changes in systems or in streams of packets flowing through the network[10, 11]. Knowledge-based systems are reliable and generate very few false positives, but they can only detect intrusions, which are similar to the ones previously encountered[12]. Such systems are powerless against new, as of yet unknown attacks, so they must be continually updated with information about new types of attacks being utilized by hackers[5]. Recently, a trend of incorporating different AI technologies into Intrusion Detection Systems (IDS) has demonstrated promising results in particular with agent-based systems[13-15].

A behavior-based IDS instead looks at user's actions, trying to perceive attacks by monitoring system or network activity and bringing attention to any activity that doesn't seem to be typical for the system or network in question. Such activities trigger an alarm, which may notify system or networking administrator that an attack may be taking place; often it is a false alarm. While false positives are very common with a behavior-based IDS, this is compensated with the ability to detect a previously unseen attack[5].

Behavior Based Intrusion Detection (BBID) is also known under such names as anomaly detection and statistical intrusion detection[16]. The first step BBIDS goes through is to learn what behavior is normal for the given system. Once a BBIDS is activated for the first time, it will monitor and log a number of parameters such as: bandwidth usage, processor and memory activity, disk usage, and other system activity over a certain period to create a baseline for what constitutes normal behavior. After the learning period is completed, activity that doesn't correspond well to the statistically normal system performance will result in an alert signal being generated. The main advantage of this type of IDS is that it dynamically adapts to new types of attacks. Because system behavior can fluctuate during use for normal reasons, it typically produces a very high number of false alarms[5].

As was previously mentioned, main advantage of behavior-based approaches is that they can detect attempts to exploit new and unforeseen vulnerabilities. They can even contribute to the automatic discovery of these new attacks. BBIDS are also less dependent on operating system-specific attack approaches. They also help detect internal-abuse types of attacks that do not actually involve exploiting any security vulnerability, but rely on privileges already possessed by the users to obtain additional control over the system. BBIDS is basically an obsessed approach: Everything which has not been seen previously is classified as some type of an attack[5].

Corresponding Author: Roman V. Yampolskiy, University at Buffalo, 2145 Monroe Ave. #4, Rochester, NY, 14618, USA. Tel: (585)269-9629

The high false alarm rate is the primary drawback of BBIDS because the entire spectrum of the behavior of the user may not be encountered during the learning phase. Since behavior can change over time, there is a need for periodic online retraining of the behavior profile. This additional training may result either in unavailability of the BBIDS or in additional false alarms being generated. The system we are trying to protect can also be under attack at the same time as the BBIDS is learning the behavioral profile. Consequently, the behavioral profile will contain intrusive behavior, which is not detected as anomalous during the utilization of BBIDS[5].

REQUIREMENTS OF A TAXONOMY

Research in security is itself an area of investigation which can benefit from a systematic classification and analysis. Some of the first attempts at analyzing state of computer security research appeared long before prevalence of the personal computer[17]. Catherine Meadows presented a taxonomy of computer security research and development intended to spot areas of research which are still relatively unexplored[18]. The proposed taxonomy includes five broad areas including: systems, policies, techniques, assurance and interaction with other system requirements all of which are further subdivide into more narrow categories.

Lundin et al. presented a survey which focuses on different issues which must be addressed in order to build fully functional and practical IDS[19]. The survey focuses on such aspects of IDS as: social aspects, foundations, data collection, detection methods, response, environment and architecture, IDS security, testing, evaluation, and operational aspects.

In general, a good taxonomy has a number of desirable properties as outlined in Hansman[20]:

- **Accepted:** The taxonomy should be structured so that it can become generally approved.
- **Comprehensible:** A comprehensible taxonomy will be able to be understood by those who are in the security field, as well as those who only have an interest in it.
- **Complete:** For the taxonomy to be exhaustive, it should account for possible attacks and provide categories accordingly.
- **Deterministic:** The procedure of classifying must be clearly defined.
- **Mutually exclusive:** Each attack is categorized into, at most, one category.
- **Repeatable** Classification should be repeatable.
- **Backwards compatible:** Existing terminology should be used in the taxonomy so as to avoid confusion and to build on previous knowledge.
- **Terms well defined:** There should be no confusion at to what a term means.
- **Unambiguous:** Each category of the taxonomy must be well defined so there is no ambiguity with respect to an attack's classification.
- **Useful:** A useful taxonomy will be able to be used in the security industry and particularly by incident response teams.

INTRUSION DETECTION SYSTEMS, TECHNOLOGIES AND PRODUCTS

Probably the largest number of surveys, taxonomies and classifications of all computer security areas reviewed in this paper is concerned with different IDS. In fact the different IDS taxonomies are so numerous that meta-studies of such classification systems began to appear[21, 22].

Debar et al. developed taxonomy which defines families of intrusion detection systems according to their properties[23]. The main categories used in their classification are detection method, behavior on detection, audit source location, and usage frequency. They have later extended their taxonomy beyond real-time intrusion detection to include additional aspects of security monitoring, such as vulnerability assessment[24].

Stefan Axelsson developed a taxonomy which consists of a classification based on detection principle and operational aspects of the IDS[25]. The detection principles are divided into anomaly, signature, and signature-inspired. The system characteristics categories considered are time of detection, granularity of data processing, source of audit data, response to detected intrusions, locus of data processing, locus of data collection, security and degree of interoperability. Author uses developed classification to survey and classify a number of research prototypes.

Lazarevic et al. developed a taxonomy of IDS based on five criteria: information source (system commands, system accounting, system log, security audit processing, network packets, application log files), analysis strategy, time aspects, architecture, and response type[26].

Many other IDS surveys and taxonomies have been put forward including:

- Allesandri et al. developed a taxonomy of IDS with respect to the analysis of activities such as attacks and other related events[27]. The attributes a classified into three categories: generic characteristics, data preprocessing, and instance analysis.
- Xiao et al. classify the architectures of IDS that have been developed for mobile ad hoc networks (MANET)[28].
- Michael Treaster describes different approaches what have been developed to share and analyze data in distributed IDS[29].

Intrusion response: Increased complexity of attacks in recent years coupled with high speed at which attacks propagate requires an automated intrusion response mechanism to be included with the modern IDS. Stakhanova et al. developed taxonomy of intrusion response systems[30]. Systems are classified based on the degree of automation, the activity of triggered response, ability to adjust, time of response, cooperation ability and response selection method.

Carver et al. proposed an intrusion response taxonomy consisting of six layers including: timing of attack, type of attack, type of attacker, degree of suspicion, attack implications and environmental constraints[31]. They suggest that a response to an attack should be customized with respect to each one of the subcategories put forward.

Jayaram et al. present a taxonomic view of network security[32]. They quantify the classes of security threats and mechanisms for meeting these security threats. They identify five ways in which network security can be compromised including: physical, system weak spots, malign programs, access rights, and communication channels.

Alarm Correlation: Many IDS are complementary to each other and are used in combination, since for different environments some approaches perform better than others. Alert correlation methods help to discern between positive and false alarms generated by such multi-IDS approaches. Zurutuza et al. present a survey of intrusion detection alarm correlation approaches[33]. Reviewed methods for alarm correlation include: probabilistic alarm correlation, method of duplicates and consequences, and predicate logic based approaches.

Immune Systems: Artificial Immune Systems (AIS) are inspired by the Human Immune System (HIS) which protects the body against damage from bacteria and viruses. It is hoped that an AIS can protect computer systems against computer viruses in a similar fashion. Dasgupta et al. present a survey of different AIS algorithms and numerous applications of this technology to science and engineering in particular to computer security, anomaly detection in data, and fault diagnosis[34]. They review in some detail computational models based on immune system principles such as: Immune Network Model and Negative Selection Algorithm as well as other less known computational models, which emulate different immunological aspects of HIS. Similarly, Aickelin et al.[35] review AIS based approaches to intrusion detection. They evaluate a number of developed systems particularly those based on: gene libraries, negative selection, clonal selection, immune memory, idotypic networks, and self-nonself detection.

Storage Systems Security: Storage networks utilized to keep and share data such as healthcare records, and financial transactions are becoming more vulnerable to security breeches. Kher et al. presented a comprehensive survey of the security services provided by the existing storage systems[36]. Such services include authentication and authorization, availability, confidentiality and integrity, key management, auditing and intrusion detection as well as usability, manageability and performance. The storage systems surveyed in the paper consist of networked file systems (Andrew file systems, self-certifying file systems, and network attached storage devices), cryptographic file systems (shared and non-shared cryptographic systems) and storage-based IDS (self-securing storage, storage-based IDS).

IDS-product review: While a great number of theoretical surveys and classification schemas of IDS have been published a much smaller effort has been devoted to the review of actual commercially available IDS. Such reviews are important for the practical utilization of IDS by network administrators and others in charge of network security.

Kathleen Jackson developed a comprehensive compilation and categorization of commercially available IDS[37]. The survey is based on published reports, product evaluations and vendor-supplied product information. Assessment of seventeen different systems is performed in terms of detection method,

suitability, flexibility, support, performance and accuracy. In a very similar work Hakan Kvarnstrom reviews a different subset of commercially available tools for detecting intrusions in computer systems and networks[38]. Systems are compared and evaluated with respect to functioning, security, architecture, performance and manageability.

In a larger study, Stefan Axelsson classifies 20 different intrusion detection systems based on taxonomy of system features developed by the author[39]. The systems are reviewed in great detail in chronological order with each review followed by the systems' evolution from the surveyor. Allen et al. presented an assessment of publicly available intrusion detection technology[40]. The report provides recommendations for IDS sponsors, users, vendors and researchers. For the IDS developers recommendations include: creation of open source signatures, utilization of distribution model similar to the one used by anti-virus community, integration of human analysis as part of event diagnosis and expanding options for capturing forensic evidence. A large number of smaller product surveys deserve to be mentioned:

- Krugel et al. survey thirteen existing IDS and describe current state-of-the art architectures and methods used to construct those systems[41].
- Teresea Lunt surveys different well known IDS from the point of view of automated audit trail analysis techniques[42].
- McAuliffe et al. performed a survey of the state-of-the-art in IDS[43].
- Peddisetty Raju overviews the state-of-the-art in IDS products and technologies in particular evaluating six commercially available intrusion detection systems[44].
- NATO research and technology organization produced a technical report on state-of-the-art IDS which includes review of some commercial and freeware products[45].

INTRUSION, ATTACKS, ATTACKERS, FLAWS AND VIRUSES

In order to improve accuracy in incident reporting, statistics, and warning bulletins Lindqvist et al. developed a classification of computer intrusions with respect to technique as well as to result[46]. Three main subclasses of intrusions are presented: bypass of intended controls, active misuse of resources, and passive misuse of resources each type of intrusion may result in exposure of data, or denial of service or erroneous output. Alternatively, Sandeep Kumar presented a classification of computer intrusions based on classifying signatures that are used to detect the exploitation or vulnerability[47].

Attackers: Intruders themselves can be classified into different types[48]:

- **External intruders** don't have any type of authorized access to the system
- **Masqueraders** use authentication of other users to obtain corresponding privileges
- **Misfeasors** those are legitimate users who have privileged access to the system and abuse it to violate security policies
- **Clandestine users** access the system with supervisory privileges and operate at a level below a normal audit mechanism, making it very difficult to detect them

Attacks: Hansman et al. propose a four dimensional vector for attack classification[20]. The first dimension being the class of an attack such as: denial of service, password attack, physical attack, or information gathering attack. Second dimension is the target of an attack such as Windows based systems. The third dimension deals with vulnerabilities and exploits that the attack uses. The fourth dimension considers any payload an attack may include such as a virus that installs a Trojan horse.

Dominique Alessandri developed a classification of attacks and a description framework for intrusion detection systems[49]. The developed method can be used by IDS designers to predict whether a given design will be able to detect certain classes of attacks. Attacks are classified according to their externally observable characteristics. The identified attack classes are then described in terms of IDS characteristics which are needed to analyze a given class of attacks.

Buhan et al. developed a meta-classification schema of attack taxonomies to provide guidance to the process of choosing the most suitable taxonomy for a security task[50]. They classify atomic taxonomies based on the grounds of distinction including:

- **The who**. Classifies attacks based on different characteristics of an attacker.
- **The how**. Groups attacks based on the attack method used.
- **The what**. Arranges attacks based on the flaw being exploited.

Buhan's meta-taxonomy uses one taxonomy from each of the identified classes and by doing so allows for

identification of a broad range of attacks[50]. Practically all of the well known different attack taxonomies[51-59] can be classified according the proposed methodology.

Vulnerabilities and Flaws: A good taxonomy of system vulnerabilities can help in detection and elimination of flaws from the current and future systems. Bishop presents taxonomy of Unix vulnerabilities classified according to the following properties[60]:

- **Nature** The type of the flaw by genesis
- **Time of introduction** When the vulnerability was introduced
- **Exploitation domain** Where the vulnerability occurs
- **Effect domain** What is affected by the vulnerability
- **Minimum number** The minimum number of components needed to exploit the flaw

Additionally Bishop et al.[61] perform a critical analysis of other vulnerability taxonomies in particular trying to understand what makes a good taxonomy. Taimur Aslam also proposes a taxonomy of security faults in the Unix operating system[62]. His taxonomy includes such categories as: operational faults, coding faults, and environment faults all of which are subdivided into additional categories. Landwehr et al. developed taxonomy of computer program security flaws based on three broad classifications, namely by: genesis, time of introduction and location[63]. A number of other less well known surveys of vulnerabilities and flaws also exist but they tend to follow similar classification approach as the ones described above[62, 64-66].

Worms, Viruses and Trojan Horses: The following definitions for different malicious software are generally accepted by the security research community[67, 68]:

- A virus is a self-replicating malicious program which relies on a careless user or other programs to replicate itself.
- A worm is a stand alone self-replicating program which uses vulnerability in the target's code to spread itself.
- Trojan horse is a program performing unknown and unwanted actions, while posing as a legitimate program. It can be equated to a non-replicating virus or a super-class to viruses and worms.

Weaver at el.[69] proposed a taxonomy of malicious worms based on target discovery and selection strategies, worm carrier mechanisms, worm activation, possible payloads, and plausible attackers who might utilize worms. Martin Karresand has developed a comprehensive taxonomy of different software weapons which he defines as "…software containing instructions that are necessary and sufficient for a successful attack on a computer system". The taxonomy consists of 15 categories, which are independent and therefore may be used together to categorize any software weapon[67, 70]. Each category is further subdivided into 2-4 subgroups making it possible to accurately classify different malware.

Deception in Cyberspace: Deception is a valuable component of information warfare, examples include many social engineering attacks such as: phishing and "Nigerian letters". Neil Rowe presents taxonomy of deception in cyberspace[71]. He enumerates the space of possible deceptions using a new approach derived from semantics in linguistics and rates appropriateness of each of the deceptions for offense and defense in cyberwar. His taxonomy includes such categories as: space, time, participant, causality, quality, and essence.

ANTI-TEMPER TECHNOLOGIES

Collberg et al. review several techniques for technical protection of software secrets which might be revealed as a result of software reverse engineering. While advocating software obfuscation as the best approach they also consider such options as sale of services instead of application, code encryption, and native code only distribution. Software obfuscation refers to making the internals of a program unintelligible to a hacker by artificially changing the structure of the program, modifying span of variables, introducing new classes and methods, and increasing the number of arguments to a method[72].

Protection of copyrighted digital material may be accomplished by digital watermarking. Digital watermarking allows incorporation of a hidden verification message to digital audio, video, or image file. Shoemaker presents a survey of techniques used for digital watermarking including spatial, frequency and wavelet domain based approaches[73].

Atallah et al. present a general survey of multiple anti-tamper technologies[74]. They review both hardware and software based methods of protecting software from unauthorized access, reverse

engineering, and violation of code's integrity. Examined hardware approaches include trusted processors, smart cards and tokens. Software methods such as encryption wrappers, code obfuscation, guarding, digital watermarking and fingerprinting are also evaluated.

EVOLUTION OF SECURITY TOOLS

New ways of defending computer systems and networks against attacks are always being introduced. However, adaptation of novel approaches is only possible if they can be thoroughly evaluated and appropriate recommendations made with regard to their use. Molsa describes taxonomy of criteria for evaluating defense mechanisms against denial of service attacks[75]. Criteria such as effectiveness during normal activity and attack, ability to fulfill requirements on application quality of service, robustness against misuse, resilience against changes in attack characteristics, configuration capabilities, and interoperability are considered.

Kaiser et al. put forth a taxonomy for a usability evaluation of security tools[76]. The proposed taxonomy ranks security functions according to the user's ability to avoid self-induced, security-critical user errors and explains possible causes of such errors. Mell et al. explore the types of performance measurements that are effective at evaluating intrusion detection systems, such as: coverage, probability of false alarms, probability of detection, resistance to attacks directed at IDS, ability to handle high bandwidth traffic, ability to correlate events, ability to detect novel attacks, ability to identify an attack, and ability to determine attack success[77].

CONCLUSIONS

As computers and computer networks infiltrate every aspect of our society computer security attracts considerable resources from both the research community and from commercial companies. In all likelihood, no IDS will ever be capable of accurately identifying every event occurring on any particular system. The increasing complexity and rapid evolution of modern computer systems prevents obtainment of absolute security. We can however hope that our intrusion detection systems will allow for reduction in the number of successful computer attacks.

In this paper we have reviewed papers which survey all aspects of computer security including attackers and attacks, software bugs and viruses as well as different intrusion detection systems and ways to evaluate such systems. The aim was to develop a survey of security related issues which would provide adequate information and advice to newcomers to the field as well as a good reference guide for security professionals. We have also developed a comprehensive review of data sources used by different IDS.

ACKNOWLEDGEMENTS

This paper is based upon work supported by National Science Foundation Grant No. DGE 0333417 "Integrative Geographic Information Science Traineeship Program", awarded to the University at Buffalo.

REFERENCES

1. Kemmerer, R.A. and G. Vigna, Apr. 2002. Intrusion Detection: A Brief History and Overview. IEEE Security and Privacy, 35(4): 27-30.
2. Lucidea, 2005. Practical Overview: Intrusion Detection Systems. Security. Available at: http://www.wlcg.com/uploadedfiles/IntrusionDetectionGuide3.pdf.
3. Janowski, M.G. and A.H. Sung, 2002. Intrusion Detection Using Neural Networks and Support Vector Machines. in Proceedings of IEEE IJCNN.
4. Novikov, D., October 2005. Neural Networks to Intrusion Detection. in MS thesis. Rochester Institute of Technology. Rochester, NY.
5. Yampolskiy, R.V. and V. Govindaraju, 17-22 April 2006. Use of Behavioral Biometrics in Intrusion Detection and Online Gaming. Biometric Technology for Human Identification III. SPIE Defense and Security Symposium. Orlando, Florida.
6. Kabiri, P. and A.A. Ghorbani, September 2005. Research on Intrusion Detection and Response: A Survey. International Journal of Network Security.
7. Jones, A.K. and R.S. Sielken, 2000. Computer System Intrusion Detection: A Survey. Computer Science Technical Report. University of Virginia.
8. Verwoerd, T. and R. Hunt, 15 September 2002. Intrusion detection techniques and approaches. Computer Communications. 25(15): 1356-1365.
9. Cannady, J. and J. Harrel, 1996. A comparative Analysis of Current Intrusion Detection Technologies. in Proceedings of Technology in Information Security Conference (TISC).

10. Bihina, M., J. Eloff, and H. Venter, January 2004. Intrusion Detection Systems: Evolution and Future Direction. Honours Thesis. University of Pretoria, South Africa.
11. Chirichiello, A., Retrieved October 7, 2006. Automated Intrusion Detection. Available at: www.dis.uniroma1.it/~dottorato/db/relazioni/relaz_chirichiello_1.pdf.
12. Blomqvist, D. and J. Skantze, 1995. Intrusion Detection: A study. Technical Report Docs 95/62 Department of Computer Systems. Uppsala University.
13. Frank, J., 1994. Artificial Intelligence and Intrusion Detection: Current and Future Directions. In Proc.17th National Computer Security Conference, National Institute of Standards and Technology. Washington,D.C.
14. Albag, H., Retrieved October 7, 2006. Network & Agent Based Intrusion Detection Systems. Available at: www.model.in.tum.de/um/courses/seminar/worm/WS0405/albag.pdf.
15. Velankar, A. A., Retrieved October 7, 2006. The Many Faces of Intrusion Detection System. Available at http://www.utdallas.edu/~axv028100/courses/cs6390/paper/IDS_paper_may01.pdf.
16. Lazarevic, A., 2003. A comparative study of anomaly detection schemes in network intrusion detection. In Proceedings of the Third SIAM International Conference on Data Mining.
17. Anderson, J.P., April 1980. Computer Security Threat Monitoring and Surveillance. James P. Anderson Co Technical report. Fort Washington, Pa.
18. Meadows, C., 1993. An outline of a taxonomy of computer security research and development. In Proceedings on the 1992-1993 workshop on New security paradigms. Little Compton, Rhode Island, United States.
19. Lundin, E. and E. Jonsson, February 2002. Survey of intrusion detection research. Chalmers University, Technical. Report.
20. Hansman, S. and R. Hunt, 2005. A taxonomy of network and computer attacks. Computers & Security, 24(1): 31-43.
21. Almgren, M., E.L. Barse, and E. Jonsson, October 15-17, 2003. Consolidation and Evaluation of IDS Taxonomies. Eighth Nordic Workshop on Secure IT systems (NordSec2003). Gjøvik, Norway.
22. Sherif, J.S. and T.G. Dearmond, 2002. Intrusion Detection: Systems and Models. Eleventh IEEE International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises.
23. Debar, H., M. Dacier, and A. Wespi, 1999. Towards a Taxonomy of Intrusion-Detection Systems. Computer Networks, 31: 805-822.
24. Debar, H., M. Dacier, and A. Wepsi, 1999. A Revised Taxonomy for Intrusion-Detection Systems. in IBM Research Report.
25. Axelsson, S., 2000. Intrusion detection systems: a survey and taxonomy. Technical Report 99-15, Chalmers University.
26. Lazarevic, A., V. Kumar, and J. Srivastava, 2005. Intrusion Detection-A Survey, Managing Cyber Threats-Issues, Approaches, and Challenges. Springer, 19-80.
27. Allesandri, D., 2001. Towards a taxonomy of intrusion detection systems and attacks. Technical Report RZ 3366, IMB Research, Zurich Research Laboratory. MAFTIA project, report D3.
28. Anantvalee, T. and J. Wu, 2006. A Survey on Intrusion Detection in Mobile Ad Hoc Networks (Chapter 7). Springer.
29. Treaster, M., December 2005. A Survey of Distributed Intrusion Detection Approaches. ArXiv Computer Science e-prints: cs/0501001. Available at: http://arxiv.org/abs/cs/0501001.
30. Stakhanova, N., S. Basu, and J. Wong, 2006. Taxonomy of Intrusion Response Systems. International Journal of Information and Computer Security.
31. Carver, C.A., 2000. An intrusion response taxonomy and its role in automatic intrusion response. Proceedings of the 2000 IEEE Workshop on Information Assurance and Security. West Point, NY, USA.
32. Jayaram, N.D. and P.L.R. Morse, 28-30 April 1997. Network security-a taxonomic view. European Conference on Security and Detection, ECOS 97. London, UK.
33. Zurutuza, U. and R. Uribeetxeberria, 1-3 December, 2004. Intrusion Detection Alarm Correlation: A Survey. In Proceedings of the IADAT International Conference on Telecommunications and Computer Networks.
34. Dasgupta, D. and N. Attoh-Okine, November 15, 1997. Immunity-based systems: a survey. IEEE International Conference on Systems, Man, and Cybernetics. Orlando, FL, USA.
35. Aickelin, U., J. Greensmith, and J. Twycross, 2004. Immune system approaches to intrusion detection - a review. Proc. of the Third International Conference on Artificial Immune Systems Number 3239 in Lecture Notes in Computer Science. Springer.

36. Kher, V. and Y. Kim, 2005. Securing distributed storage: challenges, techniques, and systems. ACM workshop on Storage security and survivability. Fairfax, VA, USA.
37. Jackson, K., 1999. Intrusion Detection System Product Survey. Technical Report: LA-UR-99-3883. Los Alamos National Laboratory, Los Alamos, New Mexico, USA.
38. Kvarnström, H., 1999. A survey of commercial tools for intrusion detection. Technical report No99-8, Chalmers University of Technology, Depart. of Computer Engineering. Sweden.
39. Axelsson, S., 1999. Research in Intrusion Detection Systems: A Survey. Technical Report No. 98-17, Dept. of Computer Engineering, Chalmers University of Technology. Göteborg, Sweden.
40. Allen, J., 1999. State of Practice of Intrusion Detection Technologies. Technical Report CMU/SEI-99-TR-028, CERT.
41. Krugel, C. and T. Toth, December 2000. A Survey on Intrusion Detection Systems. Technical reportTUV- 1841-00-11, Technical University of Vienna, Information Systems institute.
42. Lunt, T.F., October 1998. Automated Audit Trail Analysis and Intrusion Detection: A Survey. In Proceedings of the 11th National Computer Security Conference. Baltimore, MD.
43. McAuliffe, N., 3-7 Dec 1990. Is your computer being misused? A survey of current intrusion detection system technology. In Proceedings of the Sixth Annual Computer Security Applications Conference. Tucson, AZ, USA.
44. Peddisetty, N.R., 2005. State-of-the-art Intrusion Detection: Technology, Challenges, and Evaluation. in Linköping University, Department of Electrical Engineering LITH-ISY-EX-3586-2005. Available at: http://www.diva-portal.org/diva/getDocument?urn_nbn_se_liu_diva-2792-1__fulltext.pdf.
45. Coolen, R. and H.A.M. Luiijf, 2002. Intrusion Detection: Generics and State of the Art. NATO. Research & Technology Organisation. Technical Report. RTO-TR-049.
46. Lindqvist, U. and E. Jonsson, 1997. How to Systematically Classify Computer Security Intrusions. in Proc. Symp. Security and Privacy.
47. Kumar, S., August 1995. Classification and Detection of Computer Intrusions. Ph.D Dissertation Purdue University.
48. Anderson, J.P., April 1980. Computer Security Threat Monitoring and Surveillance. Technical Report. James P. Anderson Company. Fort Washington, Pennsylvania.
49. Alessandri, D., 2004. Attack-Class-Based Analysis of Intrusion Detection Systems. Ph.D Thesis University of Newcastle upon Tyne, School of Computing Science. Newcastle upon Tyne, UK.
50. Buhan, I. and P. Hartel, 2005. The state of the art in abuse of biometrics. Technical Report TR-CTIT-05-41 Centre for Telematics and Information Technology. University of Twente, Enschede.
51. Mahoney, M., September 11, 2000. Computer Security: A Survey of Attacks and Defenses. Available at: http://www.cs.fit.edu/~mmahoney/ids.html.
52. Syverson, P., 1994. A Taxonomy of Replay Attacks. Proceedings of the Computer Security Foundations Workshop VII. Franconia NH.
53. Nielson, S., S. Crosby, and D. Wallach, February 2005. A Taxonomy of Rational Attacks. In Proc. of IPTPS. Ithaca, NY.
54. Killourhy, K.S., R.A. Maxion, and K.M.C. Tan, 28 June-1 July 2004. A defense-centric taxonomy based on attack manifestations. International Conference on Dependable Systems and Networks. Pittsburgh, PA, USA.
55. Howard, J.D., 1998. An analysis of security incidents on the Internet 1989-1995, Department of Engineering and Public Policy. Carnegie Mellon University.
56. Mirkovic, J., P. Reiher, 2004. A taxonomy of DDoS attack and DDoS defense mechanisms. ACM SIGCOMM Computer Communication Review, 34(2): 39 - 53.
57. Specht, S.M. and R.B. Lee, September 2004. Distributed denial of service: taxonomies of attacks, tools and countermeasures. International Workshop on Security in Parallel and Distributed (17th ICPADS).
58. Alvarez, G. and S. Petrovic, November 2002. Encoding a Taxonomy of Web Attacks with Different-Length Vectors. Eprint arXiv:cs/0210026. Available at: http://arxiv.org/PS_cache/cs/pdf/0210/0210026.pdf
59. Abbas, A., 2005. A State of the Art Security Taxonomy of Internet Security: Threats and Countermeasures. Int'l Trans. Computer Science and Engineering, 19(1): 27-36.
60. Bishop, M., May 1995. A taxonomy of Unix system and network vulnerabilities. Technical Report CSE-9510, Department of Computer Science, University of California at Davis.

61. Bishop, M. and D. Bailey, September 1996. A critical analysis of vulnerability taxonomies. Tech. Rep. CSE-96-11, UC Davis Department of Computer Science. Available at http://www.cs.ucdavis.edu/research/tech-reports/1996/CSE-96-11.pdf.
62. Aslam, T., I. Krsul, and E. Spafford, October 1996. Use of A Taxonomy of Security Faults. 19th National Information Systems Security Conference. Baltimore, MD.
63. Landwehr, C.E., November 1993. A Taxonomy of Computer Program Security Flaws with Examples. in NRL Report 9591, Naval Research Laboratory.
64. Krsul, I., 1997. Computer vulnerability analysis thesis proposal. Technical Report CSD-TR-97-026, Computer Science Department, Purdue University.
65. Tsipenyuk, K., B. Chess, and G. McGraw, Nov.-Dec. 2005. Seven pernicious kingdoms: a taxonomy of software security errors. Security & Privacy Magazine, 3(6): 81- 84.
66. Vijayaraghavan, G. and C. Kaner, 2003. Bug Taxonomies: Use Them to Generate Better Tests. in Software Testing Analysis & Review Conference (STAR) East. Orlando, FL.
67. Karresand, M., 18-20 June 2003. Separating Trojan horses, viruses, and worms - a proposed taxonomy of software weapons. IEEE Systems, Man and Cybernetics Society Information Assurance Workshop.
68. Fagerland, S., Retrieved January 6, 2007. Norman Book on Computer Viruses. Available at: http://download.norman.no/manuals/eng/BOOKON.PDF.
69. Weaver, N., October 2003. A Taxonomy of Computer Worms. Proceedings of the 2003 ACM workshop on Rapid Malcode. Washington, DC.
70. Karresand, M., November 2002. A Proposed Taxonomy for IT Weapons. 7th Nordic Workshop on Secure IT Systems, SimoneFisher-Hübner and Erland Jonsson, Eds. Karlstad, Sweden.
71. Rowe, N., March 2006. A taxonomy of deception in cyberspace. International Conference on Information Warfare and Security. Princess Anne, Maryland, USA.
72. Collberg, C., C. Thomborson, and D. Low., July 1997. A Taxonomy of Obfuscation Transformations. Technical Report 148, Department of Computer Science, University of Auckland.
73. Shoemaker, C., 2002. Hidden bits: A survey of techniques for digital watermarking. Independent Study EED-290. Available at: http://www.vu.union.edu/~shoemakc/watermarking/watermarking.html.
74. Atallah, M.J., E.D. Bryant, and M.R. Stytz, 2004. A Survey of Anti-Tamper Technologies. The Journal of Defense Software Engineering.
75. Mölsä, J., December, 2005. December, 2005. A Taxonomy of Criteria for Evaluating Defence Mechanisms against Flooding DoS Attacks. In Proceedings of the 1st European Conference on Computer Network Defence. Pontypridd, Wales, UK.
76. Kaiser, J. and M. Reichenbach, 2002. Evaluating Security Tools towards Usable Security: A Usability Taxonomy for the Evaluation of Security Tools Based on a Categorization of User Errors. in The IFIP 17th World Computer Congress - TC13 Stream on Usability: Gaining a Competitive Edge.
77. Mell, P., July 2003. An overview of issues in testing intrusion detection systems. Technical Report NIST IR 7007, National Institute of Standard and Technology.