 doi:10.20944/preprints202206.0218.v1

Intrusion Detection Systems: A Survey and Taxonomy

Oliver Coates
Department of Computer Science,
University of Bradford
Bradford, United Kingdom
ocoates@bradford.ac.uk

***Abstract*—Intrusion Detection Systems (IDS) plays a part in modern cyber security, as a result of the increasing need for cyber security systems in the "real" world due to the increasing number of cyber attacks, more sophisticated systems are required in order to prevent these attacks - an IDS can provide this protection. Due to the sophistication of these systems, they must be properly understood, developed and analyzed - research papers can be used as a tool to improve IDS systems. This paper is composed of two main sections: a survey and a taxonomy, providing information, reviews and interpretations from relevant papers, a timeline of important papers, a discussion on the future of IDS and a classification on IDS and how to apply this.**

I. Introduction

A. Intrusion Detection Systems

In the world of cyber security, intrusion detection systems are used as a tool of detection (as the name implies) against malicious activity which might occur inside of a network, or be incoming towards a network. Due to the amount of cyber-crimes and malicious traffic being on the rise (Buil-Gil, 2020), the ever-growing need for effective cyber-security systems is required for the exponentially rising level of malicious cyber activity further exacerbated by the COVID-19 pandemic and worldwide lockdowns, encouraging more computer activity from individuals as well as organisations.

An intrusion, in terms of cyber security, could be described as some kind of malicious activity performed to an information system. This could be some kind of malware attack such as a trojan horse, a DDoS attack, a data leak event, etc... Individuals or malicious organisations or groups could perform these attacks for personal gain, monetary reasons, revenge, or for some other malicious reason, nevertheless, these attacks are considered malicious as they serve to harm an organisation and/or it's individuals. We consider an IDS as a "software or hardware system" (or a hybrid of the two) which seeks to maintain system security through the use of monitoring, identifying and detecting malicious attacks which may be incoming or occurring on or in a network.

II. A Survey and Interpretation of Intrusion Detection Systems

A. Introduction

A number of papers exist on IDS technology, including papers examining concepts relating to IDS, such as: detection methodologies, IDS classification and categorisation, issues relating to IDS, etc...

A paper published in 2012 (Liao, 2012) reviews major aspects and concepts related to IDS technology, including it's relevant counterparts (eg: IPS). A classification from this paper categorises three distinct types of IDSs: SD (signature-based detection), AD (anomaly-based detection) and SPA (stateful protocol analysis) IDS detection methodologies. SD corresponds to patterns of attacks that are known based on the knowledge of previous attacks, AD looks at deviations to normal behaviour (such as when a DOS attack occurs, making network traffic deviate from expected behaviour), finally, SPA works similar to AD IDSs, however, SPA works with "vendor-developed" protocol profiles, whereas, AD works with network or host-specific protocol profiles. Certain IDSs will utilise all three types of these methodologies. Later on we will review further advancements to these methodologies (as well as technologies).

As well as methodologies, there are also distinct types of technologies, IDS technologies are defined and summarised in table 1.

IDS Technology	IDS Description
Host-based IDS (HIDS)	Runs to collect information regarding hosts - these hosts can contain sensitive or important information. Monitors for malicious activity.
Network-based IDS (NIDS).	Analyses network traffic through the capture of network segments going through traffic, including the analysis of applications to uncover malicious patterns on a network.
Wireless-based IDS (WIDS).	Similar to NIDS, but through the analysis of wireless traffic (eg: through wireless sensors or "wireless mesh networks").
Network Behaviour Analysis (NBA).	As the name implies, this is the analysis of standard network behaviour. This involves technology similar to NIDS in which network traffic is analysed, with unnatural traffic flow being recognised.
Mixed IDS (MIDS).	A mixture of the above technologies to offer more all-round security.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 15 June 2022 doi:10.20944/preprints202206.0218.v1

Each of these methodologies and technologies have their own pros and cons, with SD having an advantage on known attacks, but suffering when unknown attacks occur. AD having an advantage on unknown or evasive attacks, but having weaker profiles due to constant changes in attacks, due to the nature of this methodology. SPA with the ability to understand protocol states, but being incredibly resources consuming. These are some of the pros and cons of each type of IDS methodology.

B. Survey and Interpretation

The review of IDS technology. Liao, 2012. (which was discussed earlier), proposed changes in terms of IDS classification, which had been identified in previous papers (Stavroulakis and Stamp (2010)), the change was in relation to IDS detection approaches, in which, the method analysed (which in turn was classified as a change from traditional views, in which anomalies and misuses were detected) was the classification of approaches in terms of: "computation-depended approach, artificial intelligence and biological concepts". The change was proposed due to difficulties in classifying detection approaches due to the difficulty in identifying the properties of detection approaches. The new classification proposed indicated a shift into "Statistics-based, Pattern-based, Rule-based, State-based and Heuristic-based" classification - this new view of classification was also backed-up through multiple intrusion detection approaches defined in a multitude of previous papers as well as taking inspiration from its predecessor (Stavroulakis and Stamp (2010)).

The technology from IDS (i.e. NIDS, NBA, etc…), while being able to capture and detect threats to a reasonable level, do have some drawbacks, such as accuracy problems, where IDS accuracy detections on false positives and false negatives has an effect on how effective the IDS technology is. However, in more recent times (Vinayakumar, et.al, 2019), DNNs (deep neural network), machine learning and artificial intelligence has been used to improve the technology in IDSs, through the analysis of various NIDS and HIDS datasets which are able to train the DNN and machine learning IDS algorithms in order to make better decisions in accordance to detection and accuracy.

The current state (excluding papers currently being worked on), shows that while the technology and methods exist to produce more effective IDSs (eg: the aforementioned DNN and machine learning IDS technology), the current major problem is finding the relevant data and datasets to produce more accurate training data for current models. Current training data available to machine learning and DNN models contain data which isn't usable or is outdated, meaning the models this is applied to can produce unreliable or inaccurate outcomes. Finally, the papers discussed above (Liao, 2012; Stavroulakis and Stamp, 2010), due to the time in which these papers were published, fall short of comprehensive reviews of certain technologies, such as the lack of proper training data for machine learning/DNN models and the solution or future of false positives/negatives which occur in many intrusion detection systems - more modern papers (Vinayakumar, et.al, 2019) do consider these issues in IDS technology, as such, we can consider that these issues in IDS technology are known to the cyber security academic and professional community.

Finally, another consideration is the current state of IoT technology. IoT technology is ever-increasing in it's prevalence in the modern world, a paper produced in 2020 (Smys, et.al, 2020) considers the ever growing prevalence of IoT devices and their need for security. This paper also considers the usage of CNN models (convolutional neural network), which utilises AI in IDS models. It is also worth noting that many papers (with the exception of Smys, et.al, 2020) do not consider multiple attacks, rather, singular attacks, limiting the range of IDS application for these papers. Smys, et.al, 2020, also considers the prevalence of false positive/negative attacks, accuracy of data, errors, etc… in it's datasets (i.e. training data for its proposed neural network model for IoT IDS system), whilst also defining a clear RNN description and explanation for it's IDS, the paper was also published recently, meaning it is also utilising current technology, therefore, you could consider this paper to be a potential leader in published IDS work - especially in relation to IoT IDS technology papers.

C. Conclusion and Future of IDS

To conclude this survey, the technology for IDS has clearly been adapted and developed over the last few decades, traditionally, IDS technology was based on the technology readily available at the time of writing, eg: 2012, where AI in cyber security was still emerging, more traditional IDS technology was primarily being used, such as virtual networks, NIDS (which could be considered inaccurate - due to the fact there are higher rates of false positives - alerting to non-existent attacks - and false negatives - letting legitimate attacks through), management and database servers, etc... While these technologies are still in usage now, we also utilize more modern technologies in IDS. The future for IDS technology is clear: DNNs, machine learning, AI and big data are crucial to developing more effective IDS technologies - better training data and ML algorithms can reduce the probability of false positives and negatives, especially with higher quality data. Aids to future developments of IDS technology will progress at a faster rate the more relevant security data is shared between trusted organisations to improve training data for machine learning algorithms and DNNs.

Finally, we could also make a prediction into the far future of IDS and cyber security in general. Recent papers (Payares, et.al, 2021) examines how quantum machine learning methods could be used in intrusion detection for detecting DoS attacks. A hybrid combination of quantum support vector machines and traditional neural networks work together in order to produce extremely accurate and practically error-less (performance rates estimated at 100%-96% - in worse-case scenarios), however, the technology for quantum computing, processing, encryption, etc… is currently still being researched and developed. In the future, prototype quantum IDS (QIDS) may be developed in order to produce extremely

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 15 June 2022 doi:10.20944/preprints202206.0218.v1

high-performance intrusion detection systems. Other advanced developments include the proposal of a "perimeter intrusion detection with a multilayer perceptron" and using quantum classifiers in order to develop more accurate and efficient intrusion detection systems (Thirumalairaj, et.al, 2020).

III. Intrusion Detection Systems: A Taxonomy

A. Background

Before we begin, the taxonomy this paper produces aims to describe, predict and explain intrusion detection systems. We produce a tool which can: describe the behaviours related to an IDS, a tool which can predict which aids in potential future classification (where all information might not be available) and, finally, explains behaviours related to IDSs. This taxonomy will also discuss, review and evaluate previous IDS taxonomies and classifications in order to understand and improve on the proposed taxonomy.

B. A Proposed Taxonomy

Previously in this paper, we briefly examined classifications of IDSs, IDS technologies and IDS methodologies. We can propose a new or, simply, improved taxonomy based on a mixture of traditional classifications combining the foundation classifications from previous decades with modern technologies, taxonomies and classifications to propose a more combined, well-rounded and modern taxonomy and classification of intrusion detection systems.

Before we lay the foundation of our proposed taxonomy, we must first take into account the previous classifications and taxonomies of IDSs. Liao, 2012, produces an overview of IDS taxonomy, in which, an IDS can be described using 4 main branches, which each go off into 3 distinct sub-branches of classification:

Intrusion Detection System	
Category	**Sub-Category**
Category	Detection Response, Granularity, Time of Detection.
Detection Strategy	Detection Methodology, Processing Strategy, Detection Discipline.
Data Source.	Data Type, Data Collection, Collection Component.
System Deployment	Technology Type, Networking Type, Network Architecture.

The above taxonomy can be used to describe IDS systems, however, this taxonomy was proposed in a paper produced in 2012, newer technologies have emerged, leaving some room for improvement with this taxonomy (eg: the considerations into DNNs, ML and big data, for example, are harder to describe within this taxonomy).

Smys, et.al, 2020. Also produces a similar taxonomy (or, rather, a classification) built specifically for IoT devices, this includes a new distinct category: "Validation Strategy" which has 4 further sub-categories: "Hypothetical", "Empirical", "Simulation" and "Theoretical", whilst also simplifying the detection strategy category and making another minor change to placement strategies which we won't consider for this taxonomy. Therefore, to consider IoT devices within our taxonomy, we will include this consideration to describe our taxonomy further. The potential drawback of using this taxonomy within our proposal is that this taxonomy was developed specifically for an IoT intrusion detection system, while systems might be similar, an IoT device will face different threats compared to "regular" organization or an individual's computer systems, as such, this might cause classification problems. However, due to the increasing amount of IoT devices, it would be unwise not to include this, at least as a consideration into the security threats faced by IoT devices.

Therefore, based on these previous classifications, we can produce the following taxonomy which states the following categories, sub-categories and descriptors (i.e. how to describe this categorical aspect of the IDS):

The following taxonomy (Table 1.0) takes a baseline taxonomy (Laio, 2012) (which could be considered a good foundation to build a modernised taxonomy) while taking into account modern concerns and technologies, such as IoT IDS systems, neural networking and machine learning.

C. Application of Taxonomy

Below annotates the described IDS taxonomy in brief detail with each category and sub-category getting a brief description as well as a description of it's properties:

Timeliness (Category - Emboldened) - Relationship between time, attacks and responses.

Detection Response (Sub-Category - Italicised) - The response to attacks the IDS detects, normally: passive responses and active responses (which can also be corrective to the attack or proactive to diverting the attack).

Frequency - The frequency in which attacks are processed by an IDS: continuously, periodically or as a "batch" (processed in bulk).

Time Consideration - The "time" an attack was detected, i.e. if the attack was detected when it happened (real-time) or post-attack.

Detection Strategy - This relates to how attacks are detected and the strategies in which attacks are detected.

Detection Methodology - The methods in which attacks are detected: anomaly, signature, specification based or a hybrid of the methods.

Architecture - The system architecture in which attacks are detected, for instance, a centralised system which processes the attacks.

Detection Discipline - How detections are based, for instance, state-based - in which detection is secure. In another case: transition-based - in which detections may go from secure to unsecure.

Self-Training - A system which trains itself to perform better (eg: improving accuracy, detecting more attacks, preventing false-positives/negatives, etc...).

Data Source - The relationship between attacks, the IDS and data-related aspects.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 15 June 2022 doi:10.20944/preprints202206.0218.v1

Intrusion Detection System (Table 1.0)		
Category	**Sub-Category**	**Descriptors**
Timeliness	Detection Response, Frequency, Time Consideration.	Detection Response - Passive Notifications, Active Reactions: Corrective, Proactive; Frequency - Continuous, Periodic, Batch;Time Consideration - Online, Real-time, Offline, Not Real-Time.
Detection Strategy	Detection Methodology, Architecture, Detection Discipline. Self-training.	Detection Methodology - Anomaly-based, Signature-based, Specification-based, Hybrid; Architecture - Centralised, Distributed; Detection Discipline - State-based, Transition-based: Non-obstructive Evaluation, Stimulating Evaluation Self-training: ANN, RNN, CNN.
Data Source	Technology, Network Type, Network Architecture.	Technology - HIDS, NIDS, WIDS, NBA, MIDS, Hybrid; Network - Wired, Wireless, Mixed; Network Architecture - Centralised, Distributed, Hybrid, De-centralised
System Deployment	Data Type, Data Collection, Collection Component.	Data Type - Logs: Sys Commands, Sys Accounting, Sys Logs, Security Logs; Application Logs, Wireless Network Traffic, Network Traffic: Packets, Segments, SNMP Data; Data Collection - Centralised, Distributed, Heterogeneous, Decentralised; Collection Component - Agent, Sensor.
Validation Strategy	Hypothetical, Empirical, Simulation and Theoretical.	Hypothetical, Empirical, Null, Simulation and Theoretical.

Data Type - The type or category of data that has been collected, this could be in the form of network traffic, logs from the system, etc…

Data Collection - How data is gathered: eg, through centralised or distributed gathering.

Collection Component - What medium was used to collect the data (eg: a sensor on a network component).

System Deployment - Related to the physical systems in which the IDS employs.

Technology Type - The type of IDS technology being deployed, for instance, a host-based IDS (HIDS).

Networking Type - The type of network the IDS will be deployed onto, for example, a wired network.

Network Architecture - The system in which attacks are detected, for example, a distributed system that monitors data from more than one system.

Validation Strategy - Description of attacks which might occur towards the IDS, which can contribute to knowing which type of IDS to deploy and the type of IDS (as it will be known what kind of attacks the IDS will be suited for).

Hypothetical - A hypothetical attack which may occur to the IDS.

Theoretical - A theoretical attack on the IDS, this differs from a hypothetical attack, in that a theoretical attack is less likely to happen, as it is only theorised.

Empirical - An attack which is likely to happen while the IDS is operating.

Simulation - A simulated attack on the IDS (eg: stress test).

Null - No attack will occur to the IDS.

IV. Conclusion

To conclude, IDS technology, while existing for decades, is almost certainly still in the process of being improved, with research and development still occurring well into the modern era. With modern cyber security threats increasing exponentially (Jang-Jaccard, et.al, 2014; Khan, et.al, 2020), the need for more advanced and sophisticated cyber security technology is ever-needed. With the current emergence of neural networking, machine learning, artificial intelligence and big data in the world of intrusion detection systems, intrusion detection system technology is almost certainly going to keep advancing.

This paper concludes based on major cited papers over the past two decades: a survey reviewing important IDS considerations and developments over the past two decades, concluding that the current state of IDS technology suffers from a lack of relevant data. Also that the future of IDS technology is likely to go into the direction of machine learning and artificial intelligence and that current developments are already being researched and developed (Vinayakumar, et.al, 2019; Smys, et.al, 2020) - which aims to improve the accuracy of IDS technology, reducing errors, recognising false positives/negatives, etc… A basic taxonomy based on earlier taxonomies (Liao, et.al, 2012; Axelsson, 2000) combined with areas from modern taxonomies and technologies (Smys, et.al, 2020; Vinayakumar, et.al, 2019) formed a foundation to produce a combined approach of both traditional and modern classification of intrusion detection systems.

References

[1] Ansam Khraisat, Iqbal Gondal, Peter Vamplew, Joarder Kamruzzaman . (2019). Survey of intrusion detection systems: techniques, datasets and challenges. Available: https://cybersecurity.springeropen.com/articles/10.1186/s42400-019-0038-7. Last accessed 07/12/2021.

[2] I. Ghafir and V. Prenosil. “Proposed Approach for Targeted Attacks Detection,” Advanced Computer and Communication Engineering Technology, Lecture Notes in Electrical Engineering. Phuket: Springer International Publishing, vol. 362, pp. 73-80, 9, 2016.

[3] Slobodan Petrović. (Unknown). Bro intrusion detection system - Principles of operation and internal structure. Available: https://www.frisc.no/wp-content/uploads/2013/02/finse2013-petrovic.pdf. Last accessed 07/12/2021.

[4] I. Ghafir, M. Hammoudeh, V. Prenosil, L. Han and R. Hegarty, K. Rabie and F. J. Aparicio-Navarro, “Detection of Advanced Persistent Threat Using Machine-Learning Correlation Analysis,” Future Generation Computer Systems, vol. 89, pp. 349-359, 2018.

[5] Hung-Jen Liao, Chun-Hung Richard Lin, Ying-Chih Lin, Kuang-Yuan Tung. (2012). Intrusion detection system: A comprehensive review. Available: http://dl-maghaleh.ir/wp-content/uploads/2016/03/order-z-1426675381-750.pdf. Last accessed 08/12/2021.
[6] I. Ghafir, J. Saleem, M. Hammoudeh, H. Faour, V. Prenosil, S. Jaf, S. Jabbar and T. Baker, "Security Threats to Critical Infrastructure: The Human Factor," The Journal of Supercomputing, vol. 74(10), pp. 1-17, 2018.
[7] Prof. Peter Stavroulakis, Prof. Mark Stamp. (2010). Handbook of information and communication security.
[8] I. Ghafir, V. Prenosil, and M. Hammoudeh, "Botnet Command and Control Traffic Detection Challenges: A Correlation-based Solution." International Journal of Advances in Computer Networks and Its Security (IJCNS), vol. 7(2), pp. 27-31, 2017.
[9] R. Vinayakumar; Mamoun Alazab; K. P. Soman; Prabaharan Poornachandran; Ameer Al-Nemrat; Sitalakshmi Venkatraman. (2019). Deep Learning Approach for Intelligent Intrusion Detection System. Available: https://ieeexplore.ieee.org/abstract/document/8681044. Last accessed 09/12/2021.
[10] I. Ghafir, V. Prenosil, A. Alhejailan and M. Hammoudeh, "Social Engineering Attack Strategies and Defence Approaches." International Conference on Future Internet of Things and Cloud. Vienna, Austria, pp. 145-149, 2016.
[11] Stefan Axelsson. (2000). Intrusion Detection Systems: A Survey and Taxonomy.
[12] Dr. S. Smys; Dr. Abul Basar;Dr. Haoxiang Wang.. (2020). Hybrid Intrusion Detection System for Internet of Things (IoT). Available: https://irojournals.com/iroismac/V2/I4/02.pdf. Last accessed 09/12/2021.
[13] E. D. Payares, J. C. Martinez-Santos. (2021). Quantum machine learning for intrusion detection of distributed denial of service attacks: a comparative overview. Available: https://www.spiedigitallibrary.org/conference-proceedings-of-spie/11699/116990B/Quantum-machine-learning-for-intrusion-detection-of-distributed-denial-of/10.1117/12.2593297.short?SSO=1. Last accessed 10/12/2021.
[14] Julian Jang-Jaccard, Surya Nepal. (2014). A survey of emerging threats in cybersecurity. Available: https://www.sciencedirect.com/science/article/pii/S0022000014000178. Last accessed 09/12/2021.
[15] Navid Ali Khan, Sarfraz Nawaz Brohi, Noor Zaman. (2020). Ten Deadly Cyber Security Threats amid COVID-19 Pandemic.
[16] Ali Movaghar. (2008). Intrusion Detection: A Survey.
[17] David Buil-Gil, Fernando Miro-Llinares, Asier Moneva, Steven Kemp, Nacho Diaz-Castano. (2020). Cybercrime and shifts in opportunities during COVID-19: a preliminary analysis in the UK. Available: https://www.tandfonline.com/doi/full/10.1080/14616696.2020.1804973. Last accessed 10/12/2021.
[18] I. Ghafir, V. Prenosil, J. Svoboda and M. Hammoudeh, "A Survey on Network Security Monitoring Systems," International Conference on Future Internet of Things and Cloud, Vienna, Austria, pp. 77-82, 2016.
[19] A. Thirumalairaj, M. Jeyakarthic. (2020). Perimeter Intrusion Detection with Multi Layer Perception using Quantum Classifier. Available: https://ieeexplore.ieee.org/abstract/document/9171159. Last accessed 09/12/2021.
[20] M. Lefoane, I. Ghafir, S. Kabir, and I. Awan, "Machine Learning for Botnet Detection: An Optimized Feature Selection Approach". International Conference on Future Networks Distributed Systems. Association for Computing Machinery, New York, NY, USA, 2021.
[21] I. Ghafir, V. Prenosil, M. Hammoudeh, T. Baker, S. Jabbar, S. Khalid and S. Jaf, "BotDet: A System for Real Time Botnet Command and Control Traffic Detection," IEEE Access, vol. 6, pp. 1-12, 2018.
[22] S. Eltanani and I. Ghafir. "Coverage Optimisation for Aerial Wireless Networks." 2020 14th International Conference on Innovations in Information Technology (IIT). IEEE, 2020.
[23] I. Ghafir, V. Prenosil, M. Hammoudeh and U. Raza, "Malicious SSL Certificate Detection: A Step Towards Advanced Persistent Threat Defence," International Conference on Future Networks and Distributed Systems. Cambridge, United Kingdom, 2017.
[24] J. Svoboda, I. Ghafir, V. Prenosil, "Network Monitoring Approaches: An Overview," International Journal of Advances in Computer Networks and Its Security (IJCNS), vol. 5(2), pp. 88-93, 2015.
[25] I. Ghafir and V. Prenosil, "Malicious File Hash Detection and Drive-by Download Attacks," International Conference on Computer and Communication Technologies, series Advances in Intelligent Systems and Computing. Hyderabad: Springer, vol. 379, pp. 661-669, 2016.