Intrusion Detection Systems

What are Intrusion Detection Systems?

An Intrusion occurs when hackers take advantage of system vulnerabilities leading to a security breach or it can be because a user downloads a virus. Thus the function of an intrusion detection system (IDS) is to monitor a network's activity for any possible intrusions that could potentially endanger the functionality of the network. For instance, if a third party were to send a virus to access a company's restricted folders, the IDS would notify the network administrator that a breach has been made. There is a key distinction between an IDS and a firewall, and that is a firewall only prevents unwanted packets from entering a private network but it does not inform the company that there is in fact a breach. An interesting comparison could be the firewall as “the lock system in a car protects the car from theft [while the IDS as] the burglar alarm that detects that the lock has been broken and alerts the owner by raising an alarm” (SANS Institute)\(^1\). Thus companies would want to install IDS' because it could help maintain the integrity of their information and they would not need employees to manually to monitor the information system.

In order to differentiate between an efficient IDS that would benefit a company and a poorly designed intrusion system, the IDS should come equipped with the following features: multiple attack stability, quick turnaround time, and maintenance of network connection.

The system should be able to withstand more than one intrusion without compromising its performance, known as multiple attack stability. If a system would slow down or collapse after detecting an anomaly then it would not be very useful for an organization, especially if an attacker was aware of the IDS’s poor performance\(^2\).

The turnaround time to detect a malicious element in the network should be short, as this would reduce the risk that the malware has already made changes to the system or retrieved valuable information. If it took days for an IDS to report an infiltration then the magnitude of damages a company has to accept would much greater than if the report was instant\(^3\).

Another feature would be that the system could detect an intrusion without switching off the network connection within the organization. It could be costly for a company to lose network connection, for

---

\(^1\) SANS Institute, "Intrusion Detection Systems: Definition, Need and Challenges."


\(^3\) Ahmed, Pal, Hossain, Bikas & Hasan, “A Comparative Study on the Currently Existing Intrusion Detection Systems”
example a bank that makes millions of transactions a day would lose all the potential revenues from
the transactions in the downtime\textsuperscript{4}.

A system that could satisfy all these requirements would be worth the investment as it would stop
cybercrime and errors from affecting the business’s normal operations.

\textbf{The Intricacies of an Intrusion Detection System}

Currently intrusion detection systems use two types of detection techniques: anomaly method or misuse
method. These detection techniques are how IDS\textsuperscript{'s} analyse information packets and determine if there is
a breach in security. The anomaly detection technique first evaluates the network under normal
circumstances and thereby creates “the profile of user behaviour or status of network traffic” (Chen, Chen
& Lin)\textsuperscript{5}. If there is any network activity that deviates from the norm, the detector would signal to the
network administrator that an attack happened. The main advantage of having an anomaly detector is
that there is a higher chance of the system detecting unknown infiltrations; however the downside is that
there are more false alarms since any changes in user behaviour would indicate an intrusion\textsuperscript{6}. Misuse
detectors focus on what they consider an intrusion based on the different attack patterns stored within the
database and match that with the network activity\textsuperscript{7}. For example, if a third party instigates a denial of
service attack on a company, a misuse detection system would pick up on the attack signature or pattern
and inform the IT administrator. As a result, there are rarely false alarms, however if there is a new virus
or code that does not match with the attack patterns of the database, the intrusion would not be noticed.

IDS\textsuperscript{'s} are also categorized into passive or active systems, which relates to how the IDS would respond to a
known intrusion. A passive system would detect the intrusion and inform the system administrator, while
an active system would take action like freezing network connections in addition to alerting the users\textsuperscript{8}. An
efficient IDS should have both aspects because some problems that can easily be resolved by the users
and thus the system should respond passively. On the other hand, if an elaborate attack affected the
company’s computer system and an intrusion detection system should actively disconnect the server to
prevent the tainting of files.

\textsuperscript{5} Chen, Chen & Lin, “An Efficient Network Intrusion Detection”
\textsuperscript{6} Chen, Chen & Lin, “An Efficient Network Intrusion Detection”
\textsuperscript{7} Zhao, Xu & Feng, “Analysis and Design for Intrusion Detection System Based on Data Mining”
\textsuperscript{8} Ahmed, Pal, Hossain, Bikas & Hasan, “A Comparative Study on the Currently Existing Intrusion Detection Systems”
The Different Types of Intrusion Detection Systems

There are three types of IDS: host based IDS (HIDS), network based IDS (NIDS), and hybrid IDS, all of which can utilize either anomaly and misuse detection techniques.9

With the HIDS, the system could be attached to a host, for example a computer, and it would analyze the data within a network. Alternatively a NIDS is connected to the network and it evaluates the network traffic as an outer layer of protection10. A hybrid IDS has elements both a HIDS and NIDS and it is meant to complement and improve the performance over the two former software.

HIDS primarily evaluates log files within the network as its primary source of data, and through collecting, decoding, and analyzing log files, it can identify many intrusions. For example, a HIDS would examine a computer's log files, which track the computer’s activity, for any irregularities. In the collection phase, the system would observe system-level logs and application logs to determine the normal operations of the computer. In decoding, both general and key information is extracted from the log files, so that in the analysis part, the IDS can compare the extracted data with an established database of rules. If there is a match, the system will prompt the user that the computer system has been infiltrated after tracking the attack11. However to cover the entire network, a HIDS must be installed in every hardware component, which costs a lot to maintain.12

A NIDS is located behind the firewall and it has a large database for identifying all types of attacks so it is typically seen as the second line of defense13. Instead of using log data, a NIDS would analyze the network traffic by using flow analysis and network elements to understand the network behaviour and normal traffic flow. However, since a NIDS has an enormous database it would require a lot of time to analyze each information packet that flows into the network. This would slow down the performance of the overall IDS.14

A hybrid IDS has the best of both intrusion software because it would collect information from monitored hosts and collect network information between computers.15 Furthermore it would have aspects of both anomaly and misuse detection techniques so that there are higher detection rates with the anomaly method and higher accuracy of the misuse method.

9 Lin, Zhang & Ou, “The Design and Implementation of Host-based Intrusion Detection System”
10 Ashoor & Gore, “Importance of Intrusion Detection System”
11 Lin, Zhang & Ou, “The Design and Implementation of Host-based Intrusion Detection System”
12 Chen, Chen & Lin, “An Efficient Network Intrusion Detection”
13 Chen, Chen & Lin, “An Efficient Network Intrusion Detection”
14 Zhao, Xu & Feng, “Analysis and Design for Intrusion Detection System Based on Data Mining”
15 Zhao, Xu & Feng, “Analysis and Design for Intrusion Detection System Based on Data Mining”
Current Trends and Issues

IDS’ have been around for a long time now for business to protect key information from being stolen or manipulated, for instance large corporations that house private information would use IDS’ to guard its data. But with the recent IT trend of cloud computing, more companies are switching from storing confidential information on hardware to the cloud. Cloud computing is where users can store or share information and resources online as it is stored within a virtual machine. As a result, the users can access their information from anywhere as long as they have internet connection. Since more businesses and individuals are using cloud computing the service providers must ensure that the cloud is secure, and thus they are using IDS’ to do so. When integrating an IDS with a cloud unit, there are several important considerations that must be deliberated.

First of all, intrusions into a cloud computing system would be much more severe because many companies would share the same server. As a result, if information leaked, it would be for multiple users and not limited to one company. This indicates that the economic loss would be much greater since more than one party would be affected. Furthermore, it is difficult to monitor and analyze log information in a cloud system because there are many users and systems connected to the same host. Therefore, it is hard to establish the normal network activity for the IDS to rely on log data to spot intrusions.

A recommended solution to these issues would be to have a multi-level hybrid IDS whereby security is divided into three levels. The reasoning behind a multi-level system is because different companies have different risks and what they need in terms of security are not the same. Companies that have deep pockets and highly confidential information would not mind paying for an advanced IDS that would protect their information. In this scenario, the high level security would be equipped with patterns of all known attacks and have anomaly detectors that can identify hostile changes in the environment. However smaller companies and individuals that do not have as much resources would prefer lower level security where the service is essentially free. For example if a student had to decide between purchasing an intrusion detection system to protect their emails or rely on Google’s technology that is free, they would opt for Google’s inherent security system. In this situation, the cloud would be equipped with lower level security, where only patterns of attacks that are most common are stored in the database.

Another universal trend is that many individuals are now equipped with Smartphones which they use to handle their everyday web browsing. With the increasing popularity of Smartphones, there are more attackers that are interested in exploiting the new technology. Despite there being existing intrusion

---

security software for Smartphones, they were not useful for the users because they could not respond to
the threats and recover the data. Thus, there is a recent trend of utilizing “a synchronized cloud-based
intrusion detection and response framework for Smartphones” (Houmansadr, Zonouz & Berhier)\textsuperscript{20}.
Rather than the user download an app that could offer intrusion detection (ID), which would take more lot
of memory, using a cloud-based IDS would allow an individual to be equipped with real-time ID without
taking up memory\textsuperscript{21}.

**Strengths and Limitations of Intrusion Detection Systems**

*Strengths*

Intrusion detection system can sift through huge volumes of data instantly and catch deviancies or
malicious elements in the system which would have taken a human counterpart many days to do the
same thing. This is an added convenience which saves users a lot of time and resources as they do not
have to hire an IT expert to evaluate the potential intrusions or go through system log files to note
irregularities.

Another strength of intrusion software is that it safeguards information and offers the company using the
software a cushion in case its firewall fails to stop the intrusion. As a result, it reduces the likelihood that
information would be lost or corrupted.

Lastly, different companies offer IDS’ at various price points so that users with different budgets can
purchase and use the software. Therefore, companies that wish to have more features and patterns
stored in the database can choose to pay more, while users that want a standard features at a lower cost
can still afford it.

*Limitations*

The biggest limitation of IDS’ is the fact that it is not 100% accurate when detecting intrusions, for
example it did not detect all intrusions or it came back with false alarms\textsuperscript{22}. The lesser of the two evils
would be false alarms because that does not affect the integrity of a company’s information; it is just
frustrating for the system administrator to sort through the false alarms. The first error is the most
dangerous because without knowing whether a system is corrupted, it is uncertain whether the
information is secure. This makes identifying the magnitude of corrupted difficult, thus making it harder to

\begin{itemize}
  \item \textsuperscript{20} Houmansadr, Zonouz & Berhier, “A Cloud-base Intrusion Detection and Response System for Mobile Phones”
  \item \textsuperscript{21} Houmansadr, Zonouz & Berhier, “A Cloud-base Intrusion Detection and Response System for Mobile Phones”
  \item \textsuperscript{22} Banerjee & Arya, “Optimizing Operating Cost of an Intrusion Detection System”
\end{itemize}
quantify the economic loss. In the end some party would be accountable for the error, whether it is investors of the company who relied on misstated financial statements, the seller of the software who got sued, or the company suffering a loss in reputation.

Hackers are constantly developing new ways to penetrate through a company’s secured network, but until the attack is unleashed and analyzed by the software designer, there is no protection against new malware. Therefore the limitation is that IDS’ cannot be updated with new attack signature until the attack has been developed.

Although using anomaly detection indicates that IDS’ can self-learn, it is limited to informing the system admin about the error or freezing the network. Therefore, it is not automated to the point where it can correct the error or contain the intrusion itself. This inherent limitation indicates that the user cannot rely on the IDS’ to fix the problem.

Off the shelve software is not easily customizable, and for companies that have specific needs, most software would not be able to meet those requirements. Therefore, unless a company internally develops the detection software or employs a third party to design a specific IDS, it will not be able to find what it is looking for.

Relevance to Accountants

A main reason why accountants would prefer companies to have intrusion detection software is because although data security protects a company’s confidential information or competitive advantage, the most relevant aspect of an IDS is that they ensure the reliability of a company’s financial statements. However, despite being automated and efficient, IDS’ lack professional judgement and the system alone cannot work towards better information security. Therefore, internal auditors should regularly assess the effectiveness of the company’s internal controls, especially those related to information security. By reviewing how a company’s information is safeguarded it could help determine if there are any areas of improvement and give recommendations to the IT department on how to improve the security. This

---

would require cooperation from the IT personnel because they are the ones receiving the feedback and implementing the chances or updating the IDS system\textsuperscript{27}.

For external auditors, when a client has installed intrusion detection software and there are documented reviews by the internal audit committee, it reduces the audit risk. The reason being the financial statements are less likely to have material misstatement due to errors and a company's controls over information security is more trustworthy. Given a lower audit risk and adequate internal controls the amount of substantive testing would decrease thereby decreasing the amount of work needed to be done on an audit.

Overall external auditors should evaluate the performance of intrusion detection systems either as part of the routine assessment of internal controls or offer it to their clients as a consultation service because it verifies the work of internal auditors and it reduces audit risk. By using the following metrics as a guide, accountants can determine if a company’s IDS is working effectively. Please note that these metrics can also be used by internal auditors to help them identify recommendations.

Accuracy\textsuperscript{28}: One method to check if a system has high accuracy is by sending non-threatening viruses into the network and seeing if the IDS can identify the intrusion. IDS’ that can detect the viruses would be more reliable than IDS’ that cannot detect them. This way an auditor can gage the accuracy rate for detecting malware and set an acceptable rate for detection based on the company’s risk profile.

Resilience\textsuperscript{29}: Auditors can perform a walkthrough to determine how an IDS will respond to an attack. As mentioned, there are two ways a system can respond: passive or active. Depending on the company’s preferences, for example when a bank’s intrusion detection system detected a denial of service attack, they would want the system to notify the IT specialist and not freeze the network, certain responses are better. Therefore when measuring how resilient a system should be, accountants need to consider the needs of the company first.

Ability to differentiate: A system’s ability to distinguish between a malicious element and a normal event must be correct\textsuperscript{30}. In the scenario where a system mistakes an intrusion to be normal then the users would suffer from loss or corrupt data. On the other hand, if a system detects a normal event to be irregular then many false alarms would be generated. Auditors can evaluate the system’s ability to

\textsuperscript{27} Steinbart, Raschke, Gal & Dilla, “The Relationship between Internal Audit and Information Security: An Exploratory Investigation”
\textsuperscript{28} Banerjee & Arya, “Optimizing Operating Cost of an Intrusion Detection System”
\textsuperscript{29} Banerjee & Arya, “Optimizing Operating Cost of an Intrusion Detection System”
\textsuperscript{30} Banerjee & Arya, “Optimizing Operating Cost of an Intrusion Detection System”
differentiate by looking at logs and checking if there were any false alarms reported by the system admin. Thus, if a system reports fewer falsehoods it would be more reliable.

Sensitivity: Systems that can detect more malicious attacks are considered to be more sensitive. However, the preferred level of sensitivity is directly related to false alarm in the sense that if a company wants more sensitive software, then it should be prepared for more false alarms. Once again, if an auditor wants to test how sensitive their client’s system is they would look at the amount of false alarms. However, the more sensitive a system does not make it superior, because the optimal sensitivity level is dependent on the client’s risk profile. For example, if the client is risk adverse, they would want a system to catch all intrusions which means they want an extremely sensitive system, and in this case the more false alarms an auditor finds the better.

One important pattern between the different metrics is that ability to differentiate is inversely correlated with sensitivity. Thus a company needs to determine the trade-off between the two metrics because it cannot have both. Auditors should evaluate the client’s acceptable level of risk and inform their client which metric is more important.

**Reasons why IDS are Relevant for C-suite Executives**

With the global trend of using paperless technology and computers being integrated with completing all major functions, there are new risks of maintaining customer privacy and ensuring data integrity. Executive officers need be well aware of these inherent risk and they should be finding ways to mitigate them. Therefore executives need to know how IDS’ and other preventative measures such as good internal controls can reduce the risk of losing information security. If executives cannot manage these risks effectively, then companies could potentially suffer a loss of reputation or their competitive advantage. For example, retail businesses store a lot of their client’s personal information, like credit card information, on their computer systems. However if the company’s system were breached and the credit card information leaked onto the internet, then the company is ultimately responsible for the cost of cancelling and reissuing the cards on half of their customers. This cost is quantifiable; however the potential costs of loss of reputation, loss of customers, and lawsuits cannot be not easily estimated.

The system breach could have been avoided if the executive officers decided to install IDS’ to protect the business from intrusions. Thus, IDS’ are relevant to c-suite executives because it can help them cope with risk.

---

31 Banerjee & Arya, “Optimizing Operating Cost of an Intrusion Detection System”
32 Kress (CA Magazine), “Is your Information Safe?”
33 Kress (CA Magazine), “Is your Information Safe?”
Management of public companies that are listed on the Toronto Stock Exchange or the New York Stock Exchange are required by National Policy 58-201 “Corporate Governance Guidelines” and SOX to sign off on internal controls and to provide reliable financial information to investors\(^{34}\). An entity’s internal controls comprise of procedures and business policies that are intended to ensure that the company achieves its objectives\(^{35}\). One goal is for the financial statements to be free of materially misstatements and as an extra step to safeguard financial statements, management should use IDS’. Having a IDS monitor accounting information means that the chance of malware changing the numbers or having employees mistreat the system is less likely.

As the guest presenter on cloud computing mentioned in his presentation, he estimates in 5 years that cloud computing would take over and users would not be downloading software anymore, but rather software is sold as a commodity. Thus, with many organizations now switching from housing servers full of information to operating on the cloud, executives that have made this decision or are thinking of making this decision need to know what IDS’ can offer. Executives are hesitant to use cloud computing because they are worried about the security of information stored on the cloud or if they can access the information. However knowledge of IDS’ and how it protects the cloud would erase the fear of security breaches and allow executives to make informed decisions.

**Conclusion**

Auditors should evaluate IDS’ because it’s an integral part of information system integrity and thus they need more knowledge about IDS’ and how clients can benefit using IDS’. It is a service that accountants should get into, because IDS’ are important for businesses because it makes financial information more reliable and it protects a company’s private information. IDS’ will continue to be popular amongst businesses because current trends are moving to cloud computing and businesses would want a cloud environment backed up by IDS’. Although IDS' are not widely used for individuals, with Smartphones containing more personal data suppliers will start making IDS’ more readily available for individuals. In the future, IDS’ will only get more complex because hackers are trying to outsmart the system while IDS’ are trying to keep up with them.

---

\(^{34}\) "Issuer Guide for Companies Operating in Emerging Markets."

\(^{35}\) ACC 650 Slides
Annotated Bibliography

Intrusion Detection System – All the articles listed below are going to be added in the final paper

<table>
<thead>
<tr>
<th>Author</th>
<th>Title of Article</th>
<th>Periodical Website</th>
<th>Vol./No./Edition</th>
<th>Year Published</th>
<th>Pages</th>
<th>Date Accessed</th>
<th>Location, database, website</th>
</tr>
</thead>
</table>

The article gives examples of what makes an efficient IDS.

1) Multiple attack stability: It should be designed to handle more than one intrusion without the effectiveness of the system being compromised.
2) The turnaround time to detect a malicious element in the network should be as short as possible, this would reduce the risk that the virus has made changes to the information system.
3) It should encompass the collaboration of a HISD and NISD to get the benefit of both types
4) An IDS should be able to detect an intrusion without a network connection termination
5) A response to an intrusion can either be passive or active, where a passive system would be good with detection the malicious data, while an active system would take action like freezing network connections. An efficient IDS set up would have both active and passive aspects.
6) The data processing should be both centralized or distributed
7) A IDS should not use a trusted network
8) If the components of an IDS are less interdependent, it would reduce the chance of a bottleneck situation
9) A system should not be hierarchical as it will take longer for the components to communicate with each other

The authors also made a comparison between the different IDS used by different organizations and gave the ability and limitation of each system.
the network. It does so in three ways, either by comparing known threat patterns or a self-learning system that identifies packets that appear to be suspicious or a programmer tells the system what is considered suspicious. Regardless, the result, the system would alert the user and they would go correct the problem. There are **three types of IDS:**

1. Host based IDS (HIDS) where the data collected is analysed within the network
2. Network based IDS (NIDS) is used for outer layer protection as it scans the network traffic for any patterns that match its database
3. Hybrid based IDS is meant to be a complementary unit for the HIDS and NIDS

<table>
<thead>
<tr>
<th>Authors</th>
<th>Title</th>
<th>Journal</th>
<th>Year</th>
<th>Pages</th>
<th>Date</th>
<th>Source</th>
</tr>
</thead>
</table>

The article provides many **metrics to measure the performance of an IDS** to determine if the operating costs of maintain an IDS are worth the benefits of having an IDS. The metrics include:

1. Accuracy: If a system is accurate at detecting malware or intrusions
2. Resilience: How an IDS will respond to an attack and if it is able to handle an attack on its own
3. Ability to distinguish between a malicious element and a normal event.
4. Sensitivity: If a system is able to detect all malicious attacks. However this is in proportion to normal behaviour, the more sensitive the system is the more false alarms

<table>
<thead>
<tr>
<th>Authors</th>
<th>Title</th>
<th>Journal</th>
<th>Year</th>
<th>Pages</th>
<th>Date</th>
<th>Source</th>
</tr>
</thead>
</table>

With the **current Smartphone trend**, many individuals are using Smartphones to handle their everyday web browsing. However with increasing popularity of Smartphones, there are more attackers that are interested in exploiting the new technology. In the past, intrusion security for Smartphones was not able to respond to the threats and recover the phone to its original settings. Thus, the authors suggest using a synchronized cloud-based intrusion detection (ID) and response framework for Smartphones. Although Smartphones are able to download third-party apps that could offer ID, it takes to too much memory, thus with a cloud-based would allow Smartphones to be equipped with a real-time IDS without the heavyweight software.

<table>
<thead>
<tr>
<th>Authors</th>
<th>Title</th>
<th>Journal</th>
<th>Year</th>
<th>Pages</th>
<th>Date</th>
<th>Source</th>
</tr>
</thead>
<tbody>
<tr>
<td>Kress, Jeff</td>
<td>Is your Information</td>
<td>CA Magazine</td>
<td>2008</td>
<td>44-46</td>
<td>May 31,</td>
<td>ProQuest</td>
</tr>
</tbody>
</table>
The reason why executive officers of retail companies should know about intrusion detection systems:

Since retail companies store a lot of their client’s personal information, such as credit card information, in their computer system, an attack on the systems would prove to be fatal. If the company’s systems were breached, they are responsible for all the costs of cancelling and reissuing of the cards on behalf on the customers, any false charges made on the card, there is potential loss of reputation, loss of customers, and lawsuits. This is all set out in the PCI’s compliance standards for data security, for example the PCI states that monitoring of the computer system should be performed using log reviews and IDS. Therefore executive should be aware of the risks and how they can mitigate those risks using IDS and other preventative measures.

The current IT trend is cloud computing, where users can shares information and resources online as it is stored within a virtual machine. When integrating an IDS with a cloud unit, there are some key considerations that should be brought to light. First, intrusions into a cloud computing system are much more severe than any other system because of the economic loss. Also, it is difficult to monitor and analyze log information in a cloud computing system because there are many users and many systems are connected to the same host OS. Thus the authors propose a multi-level IDS whereby security is divided into three levels. The high-level security will be equipped with patterns of all known attacks and a portion of anomaly detection method and this would require the largest amount of resources. While the low level security are for flexible resource management where only patterns of attacks that are common and fatal are stored, thus using less resources. Before a user can access the cloud computing system, the multi-level IDS will judge the user’s past usage history and will assign a virtual machine with the pre-set security level based on that judgement.
Log files are records the computer system’s behaviour since every action made is recorded in the log. HIDS looks at log files as its primary source of data, and by collecting, decoding and analyzing the log file, it can identify any intrusions.

The collection phase is where the IDS would examine system-level logs and application logs to determine the normal operations of the computer system.

In decoding there are two steps, the first is pre-decoding where general information is extracted from the log and second is the actual decoding where key information is extracted.

The analysis part is when the HIDS compares the log files with an established database of rules and if they match a given rule then the IDS will prompt the user of the intrusion after tracking the attack or do nothing if it is not an intrusion.

Another way to set up rules in the database is using BP neutral network analysis technology. Measures that can be used in an input value algorithm to establish a rule for intrusion detection include: Login frequency at different terminals, time of each session, passwords fails, the frequency of file read, write, create, and delete.

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="http://scholar.googleusercontent.com/scholar?q=cache:-sXGhvpYdY0J:scholar.google.com/+A+Comparative+Study+of+Related+Technologies+of+Intrusion+Detection+%26+Prevention+Systems&amp;hl=en&amp;as_sdt=1,5&amp;as_ylo=2008">http://scholar.googleusercontent.com/scholar?q=cache:-sXGhvpYdY0J:scholar.google.com/+A+Comparative+Study+of+Related+Technologies+of+Intrusion+Detection+%26+Prevention+Systems&amp;hl=en&amp;as_sdt=1,5&amp;as_ylo=2008</a></td>
<td>The article gives an overview of the different Intrusion Detection and Prevention Systems (IDPS) components, types of IDPS, and types of analysis techniques that IDPS can perform. It then recommends an IDPS called HawkEye Solution and how it works compared to other security systems.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

There is a difference between IDS and Intrusion Prevention Systems. IDS do not active respond to an intrusion, it only inform the IT administrator of the attack, while IPS will attempt to stop the attack. The common components of an IDPS are sensors, database server, management server that is a centralized device that intercepts and analyzes information from the sensors, and a console which acts as a user interface.

The most common techniques to detect an intrusion include: Artificial Neutral Networks, State Transition tables, Genetic Algorithms, Bayesian Network, and Fuzzy Logic.
Types of analysis techniques include network traffic analysis and filtering, log analysis, signature based analysis, and anomaly based.

<table>
<thead>
<tr>
<th>Authors</th>
<th>Title</th>
<th>Journal/Media</th>
<th>Volume/Issue/Year</th>
<th>Page/Ranges</th>
<th>Date</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>Zhao, Duanyang &amp; Xu, Qingxiang &amp; Feng, Zhilin</td>
<td>Analysis and Design for Intrusion Detection System Based on Data Mining</td>
<td>Second International Workshop on Education Technology and Computer Science</td>
<td>2010</td>
<td>339-342</td>
<td>May 31, 2013</td>
<td>IEEE Explore</td>
</tr>
</tbody>
</table>

Information security is not only for protecting a company’s confidential information or competitive advantage; it is also to **ensure the reliability of its financial statements**. Therefore internal auditors must review the information system security to determine if there are any areas of improvement and give recommendations on how to improve it. This would require teamwork with the IT department as they will be the one receiving the feedback and implementing changes.

Since the internal audit group should regularly assess the effectiveness of the company’s internal controls, including those pertaining to information system security, monitoring if the controls are indeed effective can improve the quality of the IDS or other measures that protect the network.

The authors of this paper believe that a hybrid IDS that uses both misuse and anomaly detection is the most effective. **A hybrid IDS contains four parts:**

1. Data warehouse technology where all the data is stored and different components of the IDS can access the data at the same time
2. Sensors include both hosts sensors (HS) and network sensors (NS). HS collect information in monitored hosts, while NS collect network connection information between computers
3. The analysis engine where the misuse and anomaly detectors find intrusions based on the patterns stored in the warehouse. Misuse detection matches current user behaviours and the system with the existing intrusion patterns, so that anything that matches is considered an intrusion. Anomaly detection first evaluates the behavioural models for users under normal circumstances and then compares the current with the behaviours.
it has identified; anything that is not consistent is considered an intrusion. The analysis engine also allows for pattern mining for unknown intrusions.

4. Alarm system which alerts the user, traces the source when necessary and documents the intrusion in the data warehouse.

Additional sources:


