Running head: INTRUSION DETECTION SYSTEMS IN HOSPITALS

Intrusion Detection Systems in Hospitals: What, Why, and Where.

Jody Barnes

East Carolina University

Abstract

With an ever increasing amount of information in hospitals stored electronically, regulations and potential threats to that information have made Intrusion Detection Systems (IDS) a necessity. In this paper we will look at three critical questions regarding the use of IDS in a hospital environment. First, we will review the types of IDS and how they work. Next, we cover why IDS is becoming a vital part of information security in hospitals. Finally, we will look at the best practices for IDS use and placement to insure maximum efficiency and security. Although electronic information in hospitals helps enhance patient care, it must be protected, and IDS is one step in the security process.

Intrusion Detection Systems in Hospitals: What, Why, and Where.

Introduction

As information systems in hospitals continue to advance and evolve, so do the threats to those systems. In today's healthcare environment, Patient Health Information (PHI) is no more than a few clicks away. The ease of access helps healthcare providers be more efficient and provide better patient care. This same access introduces risks that must be addressed to ensure that this information is protected. Not only is this protection of PHI the right thing to do, legislation such as the Health Insurance Portability and Accountability Act (HIPPA) make it mandatory.

Guarding assets such as PHI in a healthcare facility can be a very challenging task. The threats to such information come in many different forms and from various sources. Many think viruses and outside attackers are the only threats that need to be addressed; however, this is not the case and couldn't be further from the truth. Many threats often come from inside such as a user altering files and elevating permissions. As stated by McHugh (2001), "the problems posed by malicious users are rampant, and the inability of commodity operating systems to provide more that minimal protection has lead to a variety of attempts to secure computing systems through add-on or external means"(p.1). We must ensure that we look at all the different forms and directions of potential threats to our data.

In this struggle to secure our data and the systems on which it is stored, Intrusion Detection Systems (IDS) can prove to be an invaluable tool. As stated by Kemmerer, Kher, Robertson, & Vigna (2003), "the goal is to perform early detection of malicious

activity and possibly prevent more serious damage to the protected site" (p.1). By using IDS, we can potentially identify an attack and notify appropriate personnel immediately so that the threat can be contained. IDS can also be a very useful tool for recording forensic evidence that may be used in legal proceedings if the perpetrator of a breach is prosecuted. By itself, IDS does not protect resources, it does however alert personnel of the threat and allows for appropriate action to be taken.

What

Intrusion Detection Systems (IDS) are used "to monitor a resource and notify someone in the event of a specific occurrence for an appropriate response" (Abimbola, Merabti, & Qi, 2003). IDS is an alarm system and does not prevent malicious behavior or any other type of threat. The idea is that the earlier an organization is aware of a malicious attack or misuse, the better able it is to defend itself and its resources. So as stated by Allen, Christie and McHugh (2000),

> These warnings can help users alter their installations defensive posture to increase resistance to attack. In addition, an IDS can serve to confirm secure configurations and operation of other security mechanisms such as firewalls (p.1)

While IDS is not an active preventive device or complete security solution, it is a very important part of an organizations overall security plan.

Intrusion Detection Systems are categorized by where they reside and how they identify attacks. The type of IDS is determined by where it is placed, such as on a host or on the network. The different models of IDS are classified by the process the system uses

to determine an attack. The idea is to identify attack behavior without falsely identifying normal behavior as an attack. No one type of system is necessarily better or worse than any other. The organizations needs and resources will determine which type of system is appropriate.

Types of Intrusion Detection Systems

Intrusion Detection Systems can be classified into two main types: Network-based or Host-based. The type is determined by the placement of the IDS. This can either be software placed on a host or a device that resides on the network monitoring traffic flow. There are also hybrid systems emerging that are combining both host and network systems. All of these have both advantages and disadvantages; it is up to the organization to determine which is most suitable for their environment.

Network-based Intrusion Detection Systems (NBIDS) are just what the name implies, "Network Based". This system uses a device that is directly connected to a network segment to monitor traffic flows. The device uses these traffic flows as it's data source to determine whether the traffic matches a known attack signature or pattern. The three main signatures that the NBIDS uses are; attack text string, port signatures, and header signatures (Ayers & Sherif, 2003). By using the network as a data source, the NBIDS give the ability to monitor entire segments of the network for malicious behavior.

Although the NBIDS is good for detecting broad network attacks or threats, it does have some drawbacks. Because the system is monitoring the network, it may not detect isolated attacks or threats. Therefore, NBIDS isn't as effective for detecting things such as trusted-insider attacks that may only target specific devices (Ayers & Sherif,

2003). So if one individual machine is compromised, it may not be detected if it isn't passing suspicious traffic over the network. Also, if an attack is disguised in legitimate network traffic such as HTTP, FTP, SMTP, etc, it could potentially be missed. So although the NBIDS does have drawbacks, it can be an effective security monitoring device to compliment existing security measures.

Host-Based Intrusion Detection Systems (HBIDS) are another type of IDS to be considered. HBIDS typically consist of loading software on the system being monitored. The software monitors the system for changes resembling an attack or threat. HBIDS uses log files, auditing agents, communication traffic, system file integrity, suspicious processes, and user privileges to determine threats and attacks (Ayers & Sherif, 2003). Because the system is monitoring the individual host, it is effective in detecting isolated attacks including trusted-insider attacks. One drawback of the Host-based system is software must be installed and monitored on individual devices. In a large environment, this could become overwhelming (Ayers & Sherif, 2003).

Models

Intrusion Detection Systems also vary in way they determine an attacks and threat. The most prevalent models used to detect attacks include algorithms for statistical-anomaly detection, rules-based detection, and a hybrid of the two (Herringshaw, 1997). As with the type of IDS, the different models have advantages and disadvantages associated with each. The concept is to deploy the model that is most effective in the environment in which it will be used.

Statistical-anomaly model does just as the name implies, it looks for statistical abnormalities. This model runs under the assumption that abnormal behavior is indicative of a threat. The Statistical-anomaly model uses factors such as log files, audits, file/folder properties, and traffic patters to determine normal system behavior. The key to the statistical-anomaly model is what the systems considered normal behavior. Also, we must determine how much suspicious behavior must deviate for the normal profile to be considered an attack (Herringshaw, 1997). Deviation from normal activities is the basis for this IDS model.

The driving force in anomaly IDS is the use of abnormalities for detection. For this detection to occur, normal behavior must be identified. This normal behavior profile can either be manually created or can be adaptively learned. If the profile is created manually, it must be updated as the system evolves so it doesn't become outdate. Alternatively, if the profile is adaptively learned, there is an increased risk of false-positives indicating an attack when one isn't present. Because the anomaly based system works off of a normal profile to detect abnormalities, it is a very customizable model for an organization to use. Along with the customization come high false-positive rates as well as high maintenance to update the "normal" profile.

Another model of IDS commonly used is the Rule or Signature-based model. Most attacks are characterized by a sequence of events, making it is possible to create signatures to define these threats. The Signature-based system examines its data source for matches to predefined signatures or activities. The system alarms attack matches to the signatures are found in the data. This model is easier to implement and maintain than the anomaly model, although it can only detect attacks for which it has signatures. This

need for signatures causes the system to be unable to detect new threats or "Zero Day" attacks. As the system has very specific events that it is searching for, it has a very low-false positive rate in comparison to Anomaly based IDS.

Why

With an ever increasing amount of information in hospitals stored electronically, regulations and potential threats to that information have made Intrusion Detection Systems a necessity. Today, many hospitals are storing most, if not all, Personal Health Information (PHI) on electronic media for faster access to that information. With increased accessibility to PHI comes more vulnerability. We now have to do more that lock the drawer of a filing cabinet to protect this private information. Also, legislation such as the Health Insurance Portability and Accountability Act (HIPAA) are forcing healthcare institutions to secure this data. With this increased need for security, IDS can play a critical roll in the protection of this data.

Increased Threat

With more and more data being stored electronically in a hospital and given that data is becoming ever more accessible, we must identify who is accessing what information and why. As stated by Samson (2004), "is there anything more deeply personal that an individuals medical records?" This coupled with the fact that the frequency of computer intrusion is growing at an alarming rate; we must use IDS as part of our overall security plan so we are aware of threats in our environment (Ayers, Dearmond, & Sherif 2003).

The idea today in healthcare is that the more accessible we make information, the higher the level of care we are able to offer. This can be seen inside and outside of the hospital in everything from Picture Archiving Computer Systems (PACS) to remote offices using Virtual Private Networks to access patient data. As we implement these new technologies and systems, we also open new vulnerabilities that can potentially be exploited. An overall security plan is the only way for a hospital to combat these vulnerabilities, and IDS must be a major part of this plan.

HIPAA

In 1996, the Health Insurance Portability and Accountability Act (HIPAA) was enacted to protect health information by establishing transaction standards for the exchange of health information, security standards, and privacy standards for the use and disclosure of individually identifiable heath information. Entities directly impacted by this act are health plans, health clearinghouses and healthcare providers ("TLC HIPAA Overview", n.d.).

There are many rules incorporated in HIPAA, the Security Rule has the most direct impact on hospital technology systems. The rule addresses security measures such as user authentication, access controls, audit trails, controls of external links and access, physical security, systems back-up, and disaster recovery. Most notably of the legislation is to "detect and avert reasonably foreseeable errors and threats due to malicious or criminal actions, system failures, natural disasters, and errors by employees or users" (Shultz, n.d.). By using IDS in the hospital environment, we can help to ensure that these regulations and standards set forth in HIPAA are met and enforced.

The IDS can help us to answer the questions that are addressed by HIPAA. The questions are who, what, when, where, and why. In other words, according to HIPAA, we must know who accesses what, when it is accessed, where it was accessed, and why the user accessed the information. By answering these questions, we can identify whether or not a security breach has occurred and if HIPAA policy has been violated. By using IDS as part of our overall security plan, we can begin to answer these questions and help to insure compliance.

Where

One of the most critical and often underestimated aspects of IDS is where it should be placed in the organization. The goal is to determine what is being protected and then to decide what type of IDS will be most efficient and where to place it. We will look at these items for a hospital environment trying to optimize the efficiency of each system deployed. A misplaced or poorly designed IDS deployment strategy can potentially render the system worthless and ineffective.

Perimeter

Intrusion Detection Systems, in conjunction with other security appliances, are essential to help protect the hospital perimeter. There is now doubt the majority of people realizes there are potential vulnerabilities at the perimeter. The problem is that often insufficient means are used to protect this highly vulnerable aspect of the organization. Many feel as though all that is needed is a Firewall or VPN concentrator and the security work is done. This could not be further from the truth. Although these types of appliances

are necessary, we must take further steps in protecting widely exploited point in the organization. The use of IDS at the hospital perimeter is a vital part of any security plan.

A Network-based intrusion detection system would be a good fit for perimeter monitoring. The device would be placed between the security appliances such as Firewalls and the hospital network. This would give the device the ability to monitor all traffic flowing to and from the protected network. This placement also helps the NBIDS system detect attacks or exploits on normal services such as SMTP and HTTP that would typically be allowed to pass through the firewall (Pao & Wang, 2004). Also, we don't want to place the IDS outside of the security appliances used at the perimeter because these devices have a purpose so we should let them filter what they can (Lucas, n.d.). This placement would also allow us to monitor malicious activity that originates inside the trusted network such as Trojans or call-home exploits. An IDS just inside of the existing security appliances will help to compliment the measures already in place for perimeter defense.

The model of IDS used at the perimeter is also a very important decision to be made. It would be recommended to use a signature-based IDS for this implementation. Because the tremendous amount of traffic to be analyzed, we need to reduce the number of false-positives as much as possible. Otherwise, we may flood the personnel monitoring the logs of the IDS increasing the risk of alerts being disregarded; therefore, rendering the IDS useless. Although we will incur additional resources to maintain signatures and loose the ability to detect some new attacks, the trade for a reliable system is worth it.

Another possibility for perimeter IDS is the use of a system that is integrated with the security appliances protecting the perimeter. Many devices such as firewalls have the

ability to work with an external IDS to monitor traffic traversing the perimeter. This type of system would have the ability to fully utilize the potential of the perimeter security appliances. One consideration for this type of solution would be the amount of resources that may be needed to process the IDS on existing appliances.

Traffic at the perimeter should be monitored as much as effectively possible without degrading performance. Performance degradation could be in the form of desensitized personnel to overloaded resources on the IDS itself. This is a very critical point in the organization as well as the overall IDS strategy, so simple and efficient is the way to go.

Mission Critical Hosts

In a hospital environment there are servers and other devices that are necessary to the organization's functionality. It's these devices that we consider next in our IDS placement strategy. We will look at IDS options and possible solutions for identifying attacks and misuse on these devices to help ensure there normal operation.

The first thing that we need to consider is where the "Mission Critical Devices" are located. If these devices consist of severs that are consolidated into a server farm, we may consider using a Network-based Intrusion Detection System to monitor the network segment where the farm resides (Ayers & Sherif, 2003). If the devices are spread throughout the hospital, a Host-based solution may be more attractive. We must use the solution that is most appropriate to our individual organization and overall strategy.

There are a few options available for protecting server farms. A NBIDS could be deployed on the network segment. In this case, an anomaly solution may be the most

appropriate model to use. This is because the traffic on this segment should be predictable giving you the ability to make a profile or to use an adaptive profile. This system would help with intrusive or malicious behavior, but it may not be ideal for monitoring individual hosts. It doesn't allow us to monitor activities that look normal, such as a user modifying critical files. Although this solution helps, it isn't complete.

Another option for "mission critical host" is a HBIDS using anomaly protection. This would allow us to monitor individual systems no matter where they reside on the network. It also gives us the ability to monitor activity on hosts that are not network based such as a user logging into the device locally and installing or deleting files. By monitoring the system with a host-based anomaly system, we have the ability to monitor every aspect of the device. As mentioned by Lucas, "it is difficult to breach a computer or resource without affecting system files located on that machine" (p.6). This approach gives us a much more granular approach to critical host IDS as well as increased customization.

To overcome the shortcomings of each of these solutions for critical device IDS, we may choose to use combination of the two approaches. This would require that the devices reside on the same network segment. By using this type of hybrid approach, we would be able to monitor broad incidents on the network, as well as specific aspects of the individual devices. Although this approach may be more labor and resource consuming of all of the solutions, it offers a most comprehensive monitoring solution.

Non-critical devices

As technology advances continue to progress in the hospital environment, we must look at all devices as a potential threat that must be monitored. Because the "mission critical devices" are only effective if the users can access them, we must have devices, such as desktops and laptops, available for users to access the information they need. Typically, this part of the organization is overlooked in the IDS design and implementation.

To protect these non-critical endpoints, we could use either host or network based IDS. Depending on the number of devices to be monitored, NBIDS may be most effective in regards to both cost and resources. This solution would require that at least one NBDIS be deployed per network segment. Even if the environment has many segments, it will probably be fewer systems than if you were to deploy host-based systems on all of the devices. This solution also helps with threat detection when a device moves from one segment to another or an outside device is attached to the network. A standard Signature-based mode would be an appropriate approach so false-positives could be limited and the system could be easily maintained.

In some hospital environments, it may be appropriate to deploy host-based IDS on the non-critical host. This may be most appropriate for devices that are removed from the facility at times, such as laptops that are taken home. If a host-based solution is used in this case, the host has the ability to notify or log events that happen outside of the hospital. This could prove to be very useful when it is suspected that devices are being used in inappropriate ways. Although there are some benefits to a host-based solution for non-critical host, it can be very costly and hard to maintain.

The idea of protecting these hosts falls to the comment “you are only as secure as your weakest link.” In most hospital environments, that weakest link is the desktops or laptops that users work on every day. So we must address them in our overall IDS solution at some level.

Conclusion

As technology in the hospital environment continues to evolve and move forward, Intrusion Detection Systems must be an instrumental part of an organizations security posture. There is too much at risk, legally and organizationally, to not be aware of vulnerability exploits, attacks, and other threats. These are the kinds of things that we must monitor and track to ensure the integrity of our systems. Intrusion Detection is one tool that should be deployed to help maintain this integrity.

Once we have an Intrusion Detection Solution in place, we must be ever vigilant in maintaining them to insure optimal performance. IDS is a ever evolving arena so we must do everything that we can to insure what we have works as efficiently and effectively as possible. Even with the most effective system possible, we are only helping to eliminate the risk. As stated by Cuvusoglu, Mishra, and Raghunathan, “even the best IDSs could only detect about 80% of the attacks” (p.31). Great care in the selection and placement of IDS in a hospital environment must be taken to fully realize it’s benefits.

References

*Abimbola, A., Merabti, M., Qi, S. (2003). Nethost-sensor: A Novel Concept in Intrusion Detection Systems. *Eight IEEE International Symposium on Computers and Communications*, *June 2003*. (pp.232-237).

*Allen, J; Christie,A, McHugh, J. (2000, Sept/Oct). Defending yourself: The roll of Intrusion Detection Systems. *Software IEEE,* 17(5),42-51.

*Ayers, R., Dearmond, T.G., Sherif, J.S. (2003). Intrusion detection: The are and the practice, Part I. *Information Management & Computer Security*. 4,172-186.

*Ayers, R., Sherif, J.S., (2003). Intrusion detection: methods and systems, Part II. *Information Management & Computer Security.* 5, 222-229.

*Cuvusoglu, H., Mishra, B., Raghunathan, S.(2005, March). The Value of Intrusion Detection Systems in Information Technology Security Architecture. *Information Systems Research.* 16(1),28-46.

Herringshaw, C. (1997, December). Detecting Attacks on Networks. *Computers.* 30(12),16-17.

*Kemmerer, R.A., Kher, V., Robertson, W., Vigna, G. (2003). A Stateful Intrusion Detection System for World-Wide Web Servers. *Proceedings of the 19th Annual Computer Security Applications Conference, December 2003.* (pp. 34-43).

*Lucas, K. (n.d.) Low Cost Technique for Intrusion Detection. *Infosec Writers.* Retrieved March 13, 2006, from http://www.infosecwriters.com/text_resources/pdf/Low_Cost_ Intrusion_Detection.pdf.

*McHugh, John. (2001, August). Intrusion and Intrusion Detection. *International Journal*

Of Information Security, 2(1), 14.

*Pao, T., Wang, P. (2004). Netflow Based Intrusion Detection Systems. *2004 IEEE Conference on Networking, Sensing, and Control*, 2, 731-736.

Samson, R.; (2004). *Hospital Makes Network Intrusion Detection a "Critical" Componenet in its HIPAA Compliance.* Retrieved March 12, 2006, from http://www.findarticles.com/p/articles/mi_qa4137/is_200406/ai_n9427728.

Shultz, E.E. (n.d.) *The Health Insurance Portability and Accountability Act(HIPAA) and Intrusion Detection Data Correlation.* Retrieved March 11, 2006 from http://eee.high-tower.com/news_white_papers_hipaa.asp?source=news_white_papers_hipaa_home

TLC HIPAA Overview. (n.d.). Retreived November 1, 2005, from

http://www.mmcctlc.com/hipaa.htm