Network System Security Then & Now – Intrusion Detection Systems

(i) Abstract:

Securing communication in network applications involves many complex tasks. The technological advancements and the adequate use of internet needs concentration in terms of security for data transfer and communication. The isolated systems are no more considered a challenge. “Network systems is the new black”. Network systems can be connected on internet or physically. In this report I am dealing with the security issues in the network systems, especially intrusion detection systems. The paper talks about the advent of the intrusions and how they were addressed in the traditional systems, then it talks the contemporary issues in the same context bringing out solution to the challenges faced by the systems.

(ii) Introduction:

Networking has made its prominence from the age of internet and distributed systems. With the extent of networking came the challenges hand in hand hence the inevitability of security for the distributed systems rose. Applications using distributed systems are widely developed in different areas of technology. But with invent of distributed systems, we need to first understand the challenges that are to be dealt with before we could further develop systems.

In the research project, I would like to deal with the network security technique that was used to identify the breaches in the systems on a network in the beginning of the implementation of the distributed network systems.

In the course of time, the technique of identifying attacks were faded out and the new secure systems has a mechanism to avoid the intrusions. One such solution is named data networking which is included in the design of the network system. This is one way to avoid intruders into the network or loss of the secured data by unauthorized users. Although there are techniques that avoid intrusion, there can be a possibility to have attacks on the secured data or on the whole network.

The improvements in networks has reached to wireless systems and eventually wireless sensor network systems has come to everyday use as in home monitoring systems. Along with the advanced technologies the security on the systems has become inevitable. The inevitability led to the urge of employing intrusion detection systems on the wireless sensor networks. There are couple of ways that uses intrusion detection systems strategically. One of them is by distinguishing faulty data from real data. One other way is detecting which node is compromised node and remove that node from the network. But removing a node from the network system is not a viable solution.

My project paper deals with the security problems in network systems and tries to differentiate the improvements made in the field of network security. Let us for example consider an anomaly such as ‘prevention is better than cure’ which best suits the difference in strategies that were employed for security of distributed systems earlier and now. The earlier strategies were mostly concentrating on the policy and implementation of the security system once a glitch or attack is identified. The contemporary security strategies implements the firewall rather much before the attack occurred. It protects the system from any security issues. But we have to never neglect the advent of internet in the present age and has every opportunity to perform malicious activities. Hence, the system need to be prepared for both the prevention and to detect & adjust the compromised system if any attack occurs besides the firewall. Intrusion detection systems in wireless sensor networks are one such example in the present day distributed network system applications.

The paper in the later section is divided as follows: *section (iii) – Related work* discusses the concepts of papers that were selected to study. *Section (iv) – The study* projects the strengths and weaknesses of each paper and transition of technology and overcoming of weaknesses from one stage to another is analysed personally. *Section (v) – Conclusion* talks the overview of analysis and suggested the improvements to the studied concepts. *Section (Vi)- References.*

(iii) Related Work:

[1]

Security and privacy are growing concerns in the open distributed software systems community because of the Internet's rapid growth and the desire for secure transactions over it. Hence, there rose a need for secure architectures to deal with authentication and authorisation. The major concern in the network systems is malicious intrusion into the system. Those security tools and programs already existed serves the purpose of an isolated systems, but with the extent to which internet usage has increased the security breaches have also increased on a network. Intruders often compromise multiple systems when they attack a target site. At each compromised system, there may be signs of intrusive activities that agents of the respective systems discover. By gathering information from those systems (from agents of those systems), we can determine the nature of attacks against our networked systems. Therefore, the need arises for systems to cooperate with each other in order to manage such diverse attacks across networks and time.

The design and implementation discussed in the paper aims at developing a framework where an intelligent and co-operative agent communicates with the agents in other domains to share information about an intrusion. As such, this system automates the task of distributed intrusion detection while minimizing the amount of agent communication and human intervention needed.

[2]

Intrusion detection at the NIC makes the system potentially tamper-proof and is naturally extensible to work in a distributed setting. Simple anomaly detection and signature detection based models have been implemented on the NIC firmware, which has its own processor and memory.

In today's information age, where nearly every organization is dependent on the Internet to survive, it is imperative to guarantee the privacy and security of the information being exchanged. This issue has been brought further into the foreground by the recent thrust toward cyber-space security and the almost omnipresent deployment of network intrusion detection systems. The goal of an intrusion detection system is to detect inappropriate, incorrect, and unusual activity on a network or on the hosts belonging to a local network by monitoring network activity. There are two general approaches to this problem: signature detection (also known as misuse detection), where we look for patterns signalling well-known attacks, and anomaly detection, where we look for deviations from normal behaviour.

A problem with these approaches is that even if anomalous/intrusion activity is detected, one is often unable to prevent the anomalous packets from causing havoc in the form of disrupting the system and over utilizing the system CPU (e.g. via denial-of-service attacks). This paper targets the emerging application of network intrusion detection using Network Interface Cards (NICs). Specifically, we study a novel architecture for network intrusion detection using NICs, and empirically evaluate its feasibility. The primary role of NICs in computer systems is to move data between the system's components and the network. A natural extension to this role would be to actually police the packets forwarded in each direction by examining packet headers and simply not forwarding suspicious packets. The NIC-based scheme is inherently flexible, dynamically adaptive, and can work in conjunction with a host-based intrusion detection system. The host-based intrusion detection system can download new rules/signatures into the NIC on the fly, making the detection process adaptive

[3]
The Named Data Networking (NDN) architecture builds data authentication into the network layer by requiring all applications to sign and authenticate every data packet. The decision on keys and procedure of signature verification should be automated. In contrast to Traditional IP networks where applications usually rely on an additional layer (e.g., Transport Layer Security) to authenticate connections, Named Data Networking (NDN) is a proposed data-centric Internet architecture that requires every application to name and sign the produced network-level data packets and to authenticate received packets. In addition to fetching the specified keys and performing signature verification, consumers also match data and key names to determine whether the key is authorized to sign each specific data packet. To facilitate this matching process, the authors introduced the concepts of trust rules and trust schemas. A set of trust rules defines a trust schema that instantiates an overall trust model of an application. Given a trust schema that correctly reflects the trust model of the application, data producers can select (and if necessary generate) the right keys to sign the produced data automatically, and consumers can properly authenticate each retrieved data packet. Contributions as three-fold. First, a name-based trust management mechanism was identified, which is hoped not only to help secure NDN applications, but can also benefit other data-centric systems. Second, trust schema as a systematic way to define application trust models was invented and d the concept of Security design pattern to facilitate application development. Third, a prototype of trust schema interpreter was developed that has been successfully tested to automate authentication and signing process in a set of diverse NDN applications.

[4]
Wireless Sensor Networks (WSNs) were recently introduced as a new technology that combines wireless communication, computation, and sensing. Detection of masquerade attacks on WSNs requires lightweight techniques with respect to important WSN properties, like coverage, connectivity, data aggregation and specific communication patterns .The

sleep deprivation attack, the time synchronization attack , and the selective forwarding attack – some attacks that are born along with the properties Intrusion detection has been applied in WSNs to enhance their security as a second line of defense. Classical detection techniques have been employed over lightweight Intrusion. Detection Systems (IDSs), like the anomaly intrusion detection in, to detect and deter attacks that affect the normal and uninterruptible operation of WSNs. Although cryptographic mechanisms are used to protect sensor networks from masquerading attacks, attackers might compromise a node by stealing a key, and introduce afterwards faulty data from this compromised node. There are two approaches to address this problem; either distinguish faulty data from real data, or detect which node is the compromised node and exclude it from the network. In this paper the problem of detecting insider attacks in wireless sensor networks, by taking the advantages of intrusion detection when incorporating findings of game theory are discussed. Because a great number of attacks against sensor network routing originated by outsiders can be evaded by the use of authentication and encryption mechanisms , insider attacks are the most challenging and demanding to be counteracted. A game model is proposed between a potential attacker, and the intrusion detection systems used in a WSN

(iv) The Study:

In paper [1], the authors were conveying that the intrusions are to be considered as a serious challenge to the systems. The security programs and tools that were in use till then served the purpose of the isolated systems but it was the age of internet and networking of systems has come into real time scenarios. The authors identified the issue and proposed an architecture to solve the problem of intrusion on networks. The architecture works as follows: if a system is compromised by the intruders, then there may be signs left on the affected system. The architecture proposed communicates with all the neighbouring systems to find out if any system is compromised. Once an intruded system is identified, it gathers all the evidences the intruder has left on the system and analyses the issue. If an issue is previously reported by any other system then the issue will be resolved else a new solution will be proposed for the attack and this is communicated to the systems in the network.

This procedure is useful when there is no other security measure taken to avoid the intrusions. The preliminary actions on providing careful investigation of the attacks much before they were able to compromise the systems would be much useful. Sometimes it is more important to be aware of the system condition as precisely as the communication of the systems in the network. Also with the emerging trends, it is hard to hardcode the kind of attacks and their sources.

In paper [2] the limitation of the aforementioned paper can be overtaken and corrected. The authors proposed that a ‘network interface card’ (NIC) could be used to solve the security issues in the network systems. NIC is a card that is used to get connected with the network from a system. Simple anomaly detection and signature detection based models have been implemented on the NIC firmware, which has its own processor and memory. An architecture is designed by the systems that uses NIC to detect intrusions on the network much before they find a place to settle and attack the system. NIC is generally used to transfer data from an individual system to the network. Its functionality can be extended to investigate the packets coming into the network through NIC and rejecting the suspicious packets from entering the network. The malicious packets can be identified by signature detection and anomaly detection.

This NIC based intrusion detection system is overcoming the limitation of the previous problem but still has its own limitations. It was proved to be highly adaptable when used with the host based intrusion detection systems. The NICs used to check the architecture feasibility were not capable of performing floating point operations. As a result, the architecture usability restricted them to eliminate those operations or resort to estimates based on fixed-point operations. There was also an issue with non-intrusive messages that has to come into the network. The architecture needed to limit the impact on bandwidth and latency for non-intrusive messages.

In paper [3] the authors proposed an architecture that addresses the major security issue with the contemporary systems. The architecture uses 'Named Data Networking' (NDN) strategy to resolve the issue of security on the networked systems. The NDN design mandates that each network-layer data packet carries a cryptographic signature for authentication. The NDN basically requires every layer to name and sign each packet that passes through a layer, while in other techniques though uses key and signatures for security relies only on one layer for authentication and security. But the intrusion can happen at any layer. In order to automate this process of the data and key pair for authentication, it used trust schemas that were identified by trust rules to implement trust model.

This paper to a larger extent addressed the problems security in network systems, but its applications are limited. The trust model needs human intervention as those of application developers to properly define trust rules, maintain good relationship between data and keys, provide proper authentication based on the rules. Unless and until the trust schema is injected into the system to perform these actions automatically, its usefulness is not guaranteed.

In paper [4], one of the major innovations in present day technology is addressed and security issues that occur within the network are identified. The network systems focus is enhanced in the form of the 'Wireless Sensor Networks' (WSN). In the network systems, the attacks from an intruder were discussed and solutions were provided to avoid them and to deal them if attacked. The problem with WSN needing higher level security is the proximity for insider attacks occurrence. The design being complex also leads to inability of existing anti jamming techniques to be applied on the systems. Also due to the small memory capacity of the WSNs, it is hard to make use of the traditional key techniques for security. The outsider attacks were addressed with the authentication and authorisation capabilities induced into the current systems but insider attacks are to be considered. The potential attacker is an internal user of the system, who acts normally most of the times, but occasionally attacks the system by compromising a node of the WSN. According to prescriptive game theory, we examine theoretically the constructed game, to determine how players should play it, and to recommend strategies. A model was created to represent the interactions between the involved parties as an extensive form game. An insider, a Local lightweight IDS installed on a node, and a Global IDS installed on the base station of a WSN assembled the players' set of the game. Solutions of the game indicated the way the players will play the game. The game played by each node is analysed and the compromised node is identified. Recommended strategies were examined in two conflicting scenarios, one for attacking actions, and one for normal activity. As a result, it is possible to give advice that helps players to make better decisions.

Generally, the number of base stations that collect data in a sensor network, and the choice of their positions significantly influence the network's characteristics (e.g. data transfer rate). Especially because in the proposed game the incorporation of the third player, the Local IDS, has created a more complicated structure of the network, the use of more than one base stations should be considered in the future. In the proposed game model, the positioning of the base station was chosen manually or randomly, rather it could have been in a systematic automated method. The Global IDSs that were identified by the base stations were not functionally significant in the proposed model. They should in fact support the game as a distributed IDS until compromised node characteristics are identified.

(v) Conclusion:

The papers discussed above has a valuable insight into the concept of the security in the network systems, especially dealing with intrusion detection systems. Every individual concept was important considering an aspect. After the survey, I found out few parameters that are to be considered while we discuss about the intrusion detection systems for network security. First, the attack should be estimated depending on the application requirement rather than finding it and analysing it after the system is compromised. Second, while using the most famous data-key authentication methods in various systems for different security layers, one should be aware of the non-malicious data inputs and the effect of the detection system on the bandwidth of the incoming messages need to be taken care of. Third, while dealing with the more advanced concepts like WSN, the vulnerability cases are broad along with the complexity and hence the intrusion detection systems should not limit themselves to hardcoding the identified issues only. It was mentioned in the paper that the host based systems are most prevalent to the insider attacks. The process of detection should be able to differentiate threats and failures of the system and act automatically to the suspicious activities. The papers have mentioned about the malicious data, the difference between malicious data and suspicious data has also to be included in the intrusion detection systems. Finally, attacks from inside the network shouldn’t be neglected.

In the WSNs where the physical location of the sensors is at a distant location, care is needed in order to protect the network from physical and logical attacks from both internal and external sources.

(vi) References:

[1] J. M. V. Taraka Pedireddy, "A Prototype MultiAgent Network Security System," in *AAMAS '03 proceddings of second joint international conference on autonomous agent and multiagent systems*, 2003.

[2] S. P. A. G. G. L. S. N. D. P. M. Otey, " Towards NICbased Intrusion Detection," in *proceedings of KDD '03: Proceedings of the ninth ACM SIGKDD international conference on Knowledge discovery and data mining, ACM.*, 2003.

[3] Y. Y. A. A. D. Clark, "Schematizing Trust in Named Data Networking," in *Proceedings of the 2nd International Conference on Information-Centric Networking, ACM.* , 2015.

[4] I. K. P. F. T. S. K. Katsikas, "Detecting Intrusive Activities from Insiders in a Wireless Sensor Network using Game Theory.," in *In proceedings of PETRA '13: Proceedings of the 6th International Conference on PErvasive Techno*, 2015.