POSSIBLE INTRUSIONS AND THEIR DETECTION BASED ON THE PROPOSED MODEL FOR C4I SYSTEMS

Abdulhameed Alelaiwi, Muhammad Nasir

Department of Software Engineering, College of Computer & Information Sciences,
King Saud University, P.O. Box 51178, Riyadh 11543,
Kingdom of Saudi Arabia
aalelaiwi@ksu.edu.sa, mnasir@ksu.edu.sa

ABSTRACT: The protection of Command, Control, Communications, Computers, and Intelligence (C4I) systems during times of both war and peace is a major issue. There are many traditional mechanisms to provide such protection, but they have many limitations related to inaccuracy and false alarms. In this paper, we discuss possible types of attacks in the context of C4I systems, including Denial-of-Service (DoS), Distributed Denial-of-Service (DDoS), Probe, User-to-Root (U2R), and Root-to-Local (R2L) attacks, and propose a fundamental model to prevent such attacks.

Key Words: C4I, DOS, DDOS, Probe, U2R and R2L

1. INTRODUCTION

In defense systems, protecting information from the attacks of hackers is a major challenge. Different methods have been proposed for this purpose, but history has shown that they are not fully effective. Hackers are using different methods to gain access to defense systems, especially to break communication between different wings of an army or to spread unreliable information between them. During a war, such attacks can create many problems for the victim, and may influence the outcome of the war. To meet this challenge, intrusion detection systems (IDSes) for critical information systems are being designed.

In this paper, we discuss some of the most popular types of attacks on network systems. We also propose some solutions to the problem of protecting very important network systems, such as Command, Control, Communications, Computers, and Intelligence (C4I) systems, from these kinds of attacks.

It is most important that an IDS detect intrusion events in time and respond to such events immediately. Previously, most researchers identified and focused on two major approaches: anomaly detection and signature detection. Anomaly detection is based on the flagging of abnormal activities, while signature detection (also known as misuse detection) is based on the flagging of known intruder activities [1]. In signature detection, known attack patterns are represented as a library of attack signatures. It is also expected that unknown attacks similar to a known attack can be detected. Such attacks are known as neighboring attacks. In anomaly detection, any activity that deviates from the normal behavior is indicated as a foreign attack [2].

The rest of this paper is organized as follows. In Section 2, we discuss related work. In Section 3, we discuss several types of possible attacks on C4I systems. In Section 4, we present our proposed model for the prevention of such attacks. In Section 5, we present a methodology for the development of an IDS based on our proposed model. In Section 6, we describe future work. Finally, we conclude the paper in Section 7.

2. RELATED WORK

Hussain et al. [3] presented a framework for classifying Denial-of-Service (DoS) attacks based on header content, transient ramp-up behavior, and the results of novel analysis techniques such as spectral analysis. In the same work, they developed two approaches, one based on initial ramp-up transients, and the other based on spectral analysis. They also discussed some techniques useful for the development of an automated detection and response system.

In other research on DoS attacks, Akhlaghi et al. [4] suggested a queuing model for the evaluation of DoS attacks on Voice over IP (VoIP) proxies that is based on the Session Initiation Protocol (SIP). They mentioned that, with the help of their model, it is easy to develop algorithms for the calculation of stationary probability distributions.

Douligeris and Mitrokotsa [5] presented a classification of Distributed Denial-of-Service (DDoS) attacks, and developed a mechanism for defending against such attacks. They also identified advantages and disadvantages of each attack and defense category.

Chang [6] described different DDoS attack methods, presented an evaluation and systematic review of existing defense systems, and discussed a longer term solution, dubbed the internet firewall approach, based on the interception of attack packets in the Internet core before they reach the victim.

Beghdad [7] has done some interesting work on User-to-Root (U2R) attacks, focusing on the detection of such attacks. He formulated the problem of intrusion detection as a Linear Programming System (LPS) for (i) checking whether an unknown behavior is similar enough to a known behavior to be regarded as an attack, and (ii) identifying the class of attacks to which a detected attack belongs.

Yeung and Chow [8] proposed a novelty detection approach for the collection and classification of intrusion data. They suggested building an IDS using normal data through Parzen-window estimators with Gaussian kernels. Experiments showed that the approach can be suitable for

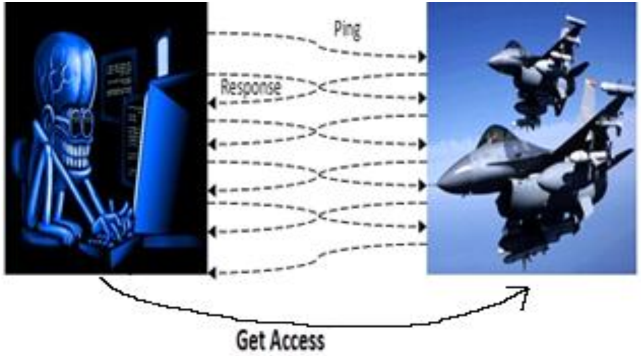

Figure 1 shows a hacker trying to access a jet's system.

intrusion detection applications in a continuously changing network environment.

Lazarevic et al. [9] conducted a comparative analysis of anomaly detection schemes. They evaluated a DARPA 1998 data set including network connection and real network data. The results of the evaluation showed that some anomaly detection schemes appear to be very promising as far as their ability to detect novel intrusions is concerned.

Tagra *et al.* [10] studied the Gossamer protocol for the prevention of DoS attacks by de-synchronization on RFID systems. They also presented a novel technique that extends the Gossamer protocol for the prevention of DoS attacks in general.

Finally, in other important work, Saghar *et al*. [11] developed a formal framework that can automatically verify different wireless routing protocols against DoS attacks. They applied their framework to the secure ad-hoc routing protocol ARAN. They tested the framework, and traced why and how attacks were successful.

3. POSSIBLE ATTACKS ON C4I SYSTEMS

There are many types of possible attacks on network systems such as C4I systems. As C4I systems are very critical and contain very sensitive information, it is most important to protect them from unauthorized access or use. Some common types of attacks on C4I systems are explained below.

DoS attacks are the most popular attacks on C4I systems. We consider three types of DoS attacks. First, in Ping flooding attacks, hackers send a ping request packet to a broadcast network address where there are many hosts. The packet contains the IP address of the computer to be attacked. As the ping request packet passes through the network, computers in the network respond with ping replies to the computer under attack. The computer under attack is flooded with ping responses, and this interrupts or even terminates its operation on the network. Second, in Smurf attacks, a ping request with a spoofed sending address is sent to a broadcast network address, with the intention of causing so many ping replies to be sent to the computer under attack that it is unable to process the replies [12]. Third, in Teardrop attacks, a normal packet is sent along with a second packet that has a fragmentation offset claiming to be inside the first fragment. This may cause the computer under attack to experience a buffer overflow and possibly crash [13].

As an example of a DoS attack, **DDoS** attacks involve a combination of DoS attacks staged by multiple hosts. As a DDoS attack has multiple sources, it cannot be prevented purely by means of filtering a source IP address. Bandwidth attacks [14, 25] are examples of DDoS attacks. DDoS attacks are very difficult to prevent. Primarily, this is due to the number and diversity of the attacking computers, as well as the variety of methods of attack. Attackers overload the victim's computer resources by flooding them with traffic.

It is very important to understand the difference between DoS attacks and DDoS attacks. If an attack is generated by a single host, then it would be classified as a DoS attack. If an attacker uses multiple systems simultaneously to launch Smurf attacks against a remote host, then this kind of attack would be classified as a DDoS attack. By adding more machines, an attacker can easily increase the potency of an attack.

Figure 2 shows an example of a DDoS attack.

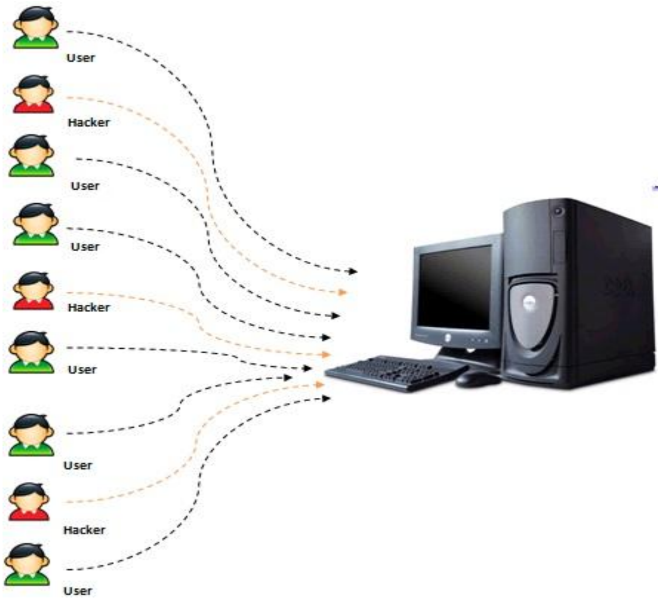

Figure 2 Example of a DDoS attack

Probing is another type of possible attack on C4I systems. It involves discovering the algorithms and parameters of the system itself. An intruder acquires this knowledge through interaction with the system itself. For this purpose, the intruder uses different tools, such as ipsweep, portsweep, and Nmap. Through probing, an attacker attempts to gather information about the available machines and services of a system in order to exploit them [15]. After breaching the current security mechanisms of the system, the intruder attempts to discover information about the system and its running programs. After identifying known or probable weak points in the system, the intruder tries to gain access to a computer and its files using either a DoS attack or a DDoS attack. Figure 3 shows an example of visual probing.

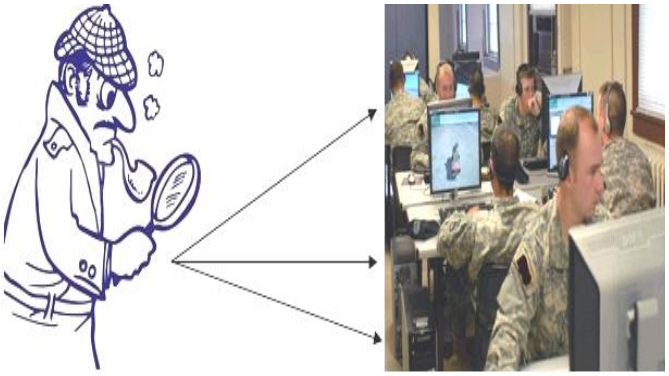

Figure 3 Example of a probing attack

Figure 4 Example of a U2R attack

In **U2R** attacks, intruders first try to obtain simple user privileges, and then they try to exploit various security flaws to gain root access [16]. For example, using Loadmodule, an attacker can easily exploit a flaw in Sun Operating System 4.1, and dynamically load modules to obtain root privileges. In some Perl implementations, there is a bug that allows any user to obtain root privileges. When an attacker obtains administrator access, he or she can easily disseminate unreliable information between different army wings; this is very dangerous, especially during a war. The attacker can even get information about the army's plans during the war. Figure 4 shows a normal user of a system trying to obtain access to the system as an administrator.

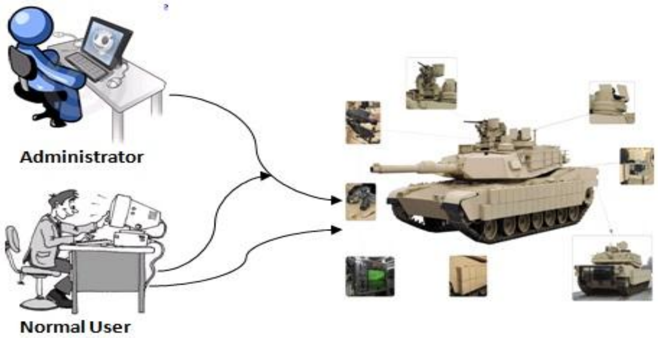

Figure 5 Example of a R2L attack

Remote-to-Local (R2L) attacks involve unauthorized access from a remote machine. The intruder uses many tools and techniques, such as IMAP, FTP write, Warezmaster, WarezClient, and the guessing of passwords. For example, the intruder might exploit a bug in the authentication procedure of an IMAP server that causes a buffer overflow and allows the intruder to obtain root privileges. The R2L category of attacks includes the most diverse set of attacks in terms of attack implementation, execution, and dynamics. R2L attacks may be distinguished in terms of their signatures and the hosts against which they are executed [17]. R2L attacks usually involve FTP servers. Therefore, they may potentially be used to corrupt or delete information for army wings.

4. PROPOSED MODEL

As shown in Fig. 6, our proposed model for the prevention of attacks on C4I systems consists of three parts: Input, Processing, and Description. The Input part involves the capturing of communication packets; i.e., it involves the use of a packet-capture engine. The packet-capture engine may be developed using WINCAP, JCAP, or JpcapDumper [26]. The Processing part involves the preprocessing of captured packets, and the classification of packets as normal or intrusive. The Processing part may be developed using soft computing techniques, which are currently hot topics in intrusion detection. The Description part may be passive or active. If it is active, it involves the prevention of intrusive packets or connections. If it is passive, it simply involves the generation of an alarm.

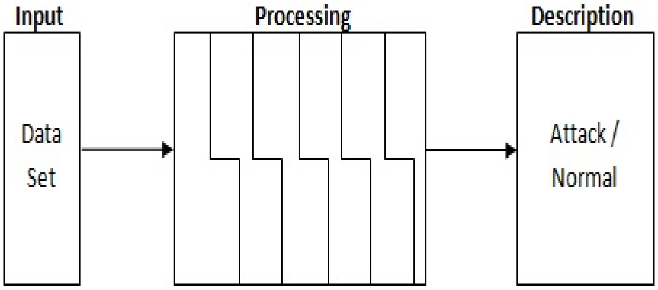

Figure 6 Proposed model for the prevention of attacks on C4I systems

5. METHODOLOGY

Our methodology for the development of an IDS for C4I systems is divided into several phases; each one is concerned with precise goals relevant to the accomplishment of the key objective. These phases are described as follows.

5.1 Selection of dataset for experiments

The capability of the intrusion detection mechanism depends on the dataset. The more accurate the training data, the better the performance of the trained system. Hence, the collection of data for training and testing is of critical importance [18-21]. Therefore, in this phase, we will discuss different issues related to obtaining a dataset for our experimental purposes.

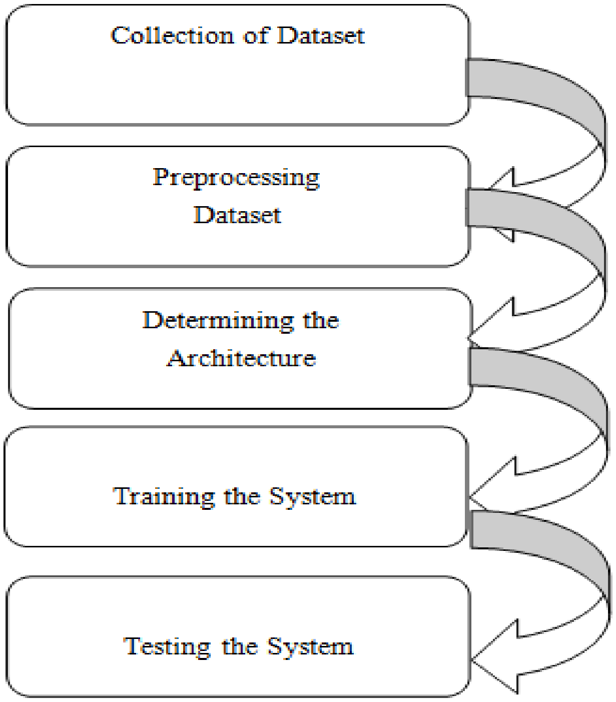

Figure 7 Phases of the methodology

Specifically, we will address the following question: Which dataset is the best for our purposes, and why?

5.2 Pre-processing of the dataset

The selected dataset will be processed so that it can be given as input to the classifier. In this phase, we will apply techniques such as PCA, *k*-dimensional scaling, *k*-means clustering, self-organizing maps, and Kernel PCA for transformation, and techniques such as genetic algorithms, greedy search, back elimination, and memetic algorithms for the selection of an optimal feature set for our proposed system [21-24].

5.3 Classification approach

After the selection of features, the next phase is determining the classification approach. We use neural networks for classification due to their proven ability, and both approaches were applied and tested in different scenarios to compare their performance [19,21-25].

5.4 Training the system

The next phase involves training the system. During training, we have both input patterns and desired outputs related to each input packet. Further, we divide the dataset into (i) a cross-validation dataset, (ii) a test dataset, and (iii) a training dataset, so that we may achieve better performance of the developed system [22-23]. The aim of the training is to minimize the error in the output produced by the system. In order to achieve this goal, weights are updated by carrying out certain steps known as training.

5.5 Testing the system

After training, the weights of the system are fixed, and the performance of the system is evaluated. Testing the system involves a verification step and a generalization step. In the verification step, the system is tested against the training data. The aim of the verification step is to test how well the trained system has learned the training patterns in the training dataset. In the generalization step, testing is conducted with data that was not used in training. The aim of the generalization step is to measure the generalization ability of the trained network [1, 20, 21]. After training, only the feed-forward phase of the computation is executed. For this purpose, we use a production dataset that has input data but no desired data.

6. FUTURE WORK

Following the methodology described in the previous section, we intend to develop an IDS for the protection of C4I systems against DoS, DDoS, probing, U2R, and R2L attacks.

7. CONCLUSION

C4I systems are very important for any defense and civil department, so their protection is very necessary. Damage to such systems could lead to defeat in war or failure of mission in peace situations. In this paper, we described various types of attacks that can cause damage to C4I systems in both war and peace situations, including DDoS, DoS, probing, U2R, and R2L attacks. We also proposed a fundamental model for the prevention of such attacks. Furthermore, based on this model, we described a methodology for the development of an IDS for C4I systems. We will attempt to carry out this methodology in future work.

ACKNOWLEDGMENT

The authors wish to thank the Research Center in the College of Computer and Information Sciences, King Saud University for funding and support of this work.

REFERENCES

1. Axelsson, S., “Intrusion Detection Systems: A Survey and Taxonomy”, Technical Report, Department of Computer Engineering: Chalmers University of Technology, Goteborge, Sweden, March 2000.
2. Labib, K. and Vemuri, V.R., “Detecting Denial-of-Service and Network Probe Attacks Using Principal Component Analysis”, *3rd Conference on Security and Network Architectures*, 2004.
3. Hussain, A. Heidemann, J. and Papadopoulos, C., “A Framework for Classifying Denial of Service Attacks”, *Proceedings of the 2003 Conference on Applications, Technologies, Architectures, and Protocols for Computer Communications, ACM SIGCOMM*, pp. 99-110, 2003.
4. Akhlaghi, A., Adibnia, F. and Shirali-Shahreza, M.H., “A queue-based analysis for Denial of Service attacks on Voice over IP proxies”, *International Symposium on Telecommunications*, pp. 19-24, October 2008.
5. Douligeris, C. and Mitrokotsa, A. “DDoS attacks and defense mechanisms, classification and state-of-the-art”, *The International Journal of Computer and Telecommunications Networking*, **44**(5), 2004.
6. Chang, R.K.C., “Defending against flooding-based distributed denial-of-service attacks: a tutorial”, *IEEE Communication Magazine,* **40**(10), 42-51(2002).
7. Beghdad, R., “Efficient deterministic method for detecting new U2R attacks”, *Journal of Computer Communications*, **32**(6), 1104-1110(2009).
8. Yeung, D.-Y. and Chow, C., Parzen, “Window Network Intrusion Detectors”, *Proceedings of the 16th International Conference on Pattern Recognition*, **4**, 385-388(2002).
9. Lazarevic, A., Ozgur, A., Ertoz, L., Srivastava, J. and Kumar, V., “A comparative study of anomaly detection schemes in network intrusion detection”, *Proceedings of the Third SIAM International Conference on Data Mining*, **3**, 25-36(2003).
10. Tagra, D., Rahman, M. and Sampalli, S., “Technique for preventing attacks on RFID systems”, *International Conference on Software, Telecommunications and Computer Networks*, pp. 6-10, November 2010.
11. Saghar, K., Henderson, W., Kendall, D. and Bouridane, A., “Applying formal modelling to detect DoS attacks in wireless medium”, *7th International Symposium on Communication Systems Networks and Digital Signal Processing*, pp. 896-900, September 2010.
12. Network and Computer Security Tutorial, http://www.comptechdoc.org/independent/security/recommendations/secattacks.html (Webpage accessed on February 2012).
13. *Patrikakis, C. Masikos, M. and Zouraraki*, O., “Distributed Denial of Services Attacks”, *The Internet Protocol Journal*, **7**(4), December 2004.

14. Azrina, R. and Othman, R., “Understanding the Various Types of Denial of Service Attack”, *Business Week Online,* 2000.
15. Ben Amor, N., Benfarhat, S. and Elouedi, Z., “Naive Bayes vs decision trees in intrusion detection systems”, *Proceeding of the 2004 ACM Symposium on Applied Computing*, pp. 420-424, 2004.
16. Bahrololum, M., Salahi, E. and Khaleghi, M., “An Improved Intrusion Detection Technique based on two Strategies Using Decision Tree and Neural Network”, *Journal of Convergence Information Technology*, **4**(4), December 2009.
17. Sabhnani, M. and Serpen, G., “KDD Feature Set Complaint Heuristic Rules for R2L Attack Detection”, *Proceedings of Security and Management*, pp. 310-316, 2003.
18. Ahmad, I., Abdullah, A.B. and Alghamdi, A.S., “Application of artificial neural network in detection of DOS attacks”, *Proceedings of the 2nd International Conference on Security of Information and Networks*, ACM, New York, pp. 229-234, October 2009.
19. Ahmad, I., Abdullah, A.B. and Alghamdi, A.S., “Application of Artificial Neural Network in Detection of Probing Attacks”, *IEEE Symposium on Industrial Electronics and Applications (ISIEA 2009)*, Kuala Lumpur, Malaysia, pp. 557-562, October 2009.
20. Ahmad, I., Abdullah, A.B. and Alghamdi, A.S., “Remote to Local Attack (R2L) Detection Using Supervised Neural Network”, *IEEE International Conference for Internet Technology and Secured Transactions (ICITST)*, London, pp. 1-6, November 2010.
21. Ahmad, I. 2012. *Feature Subset Selection in Intrusion Detection*. LAMBERT Academic Publishing.
22. Ahmad, I., Abdullah, A. and Alghamdi, A., “Towards the Selection of Best Neural Network System for Intrusion Detection”, *International Journal of Physical Sciences*, **5**(12), 1830-1839(2010).
23. Ahmad, I., Abdullah, A., Alghamdi, A. and Hussain, M., “Optimized Intrusion Detection Mechanism Using Soft Computing Techniques”, *Telecommunication Systems*.
24. Ahmad, I., Abdullah, A.B., Alghamdi, A.S., Hussain, M. and Nafjan, K., “Intrusion Detection Using Feature Subset Selection based on MLP”, *Journal of Scientific Research and Essays*, **6**(34), 6804-6810(2011).
25. Ahmad, I., Abdullah, A.B., Alghamdi, A.S. and Hussain, M., “Distributed Denial of Service Attacks Detection Using Support Vector Machine”, *Information*, **14**(1), 127-134(2011).
26. Ahmad, I., Swati, S.U. and Mohsin, S., “Intrusion Detection Mechanism by Resilient Back Propagation (RPROP)”, *European Journal of Scientific Research*, **17**(4), 523-530(2007).