Deceptive Attacks and Anomalies Detection Using Honeypot Enabled Networks

Nimitha Mary Mohan[1], Kalimuthu M[2]

[1]M.Tech. Scholar, Department of Computer Science & Engineering, Believers Church Caarmel Engineering College
Kerala, India
nimithamary [at]gmail.com

[2]Guide, Department of Computer Science & Engineering, Believers Church Caarmel Engineering College
Kerala, India

Abstract: ***In current world, interchanges innovations and leaps forward in data prompt an ever increasing number of gadgets of each possible sort being associated with the Internet. This likewise reinforces the requirement for guarantee against digital assaults. Any gadgets with a remote association could be powerless against harmful hacking attempts. Then, honey pot-based deception mechanism is one of the strategies to guarantee security for present day organizes in the Internet Things. In this paper, safeguarding against attacks in honey pot based systems is finished by taking a glance at a game theoretic model of deception including an attacker and a defender. The attacker may attempt to deceive the safeguard by utilizing diverse kinds of attacks running from a suspicious to an apparently ordinary action, while the defender thus can make utilization of honey pots as an instrument of misleading to trap attackers.***

Keywords: Networks, security, attacks, honey pot

1. Introduction

The security of the system starts with authentication, normally with a username and a secret word. An inconsistency based interruption identification framework may likewise screen the system like wire shark activity and might be logged for review purposes and for later abnormal state investigation. A honey pot can likewise coordinate an aggressor's consideration far from honest to goodness servers. A honey pot urges assailants to invest their opportunity and vitality on the fake server while diverting their consideration from the information on the genuine server. They are physical or virtual computer systems that imitate actual devices and provide heavy monitoring and activity logging, which helps wasting attackers' time and resources and allows defender to study the attacks and devise countermeasure. Honey pots are examples of deception, a classic strategy in warfare where one party intentionally misleads the other into taking actions in one's favor [1]. Smart attackers are also constantly trying to avoid being detected with stealthy deceptive attacks [2].Hidden attacks may appear normal and are hard to recognize [3]. In the long term, since attacker and defender may change their strategies based on their assessments of the play history, a repeated game version enables players to update their beliefs under Bayes rule. Various steps involved in this paper is shown in the figure below:

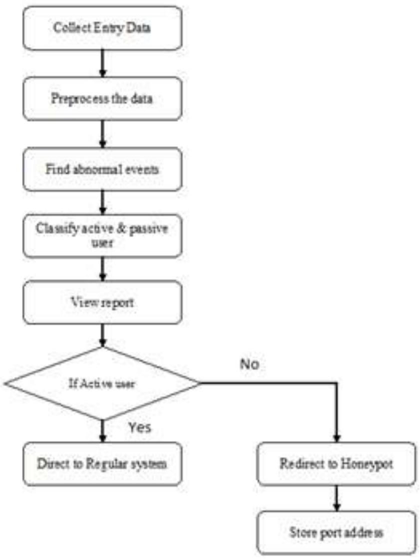

Figure 1: Flow chart showing the processes described in this paper

2. Description of the System

Current the internet in the IoT worldview all the time comprises of systems, in which various shrewd yet conceivably helpless articles are conveyed and Internet-associated. For instance, brilliant family unit gadgets, electric meters, therapeutic wearable gadgets or remote sensors are among the central competitors. To give insurance against potential assaults, multi-layer safety efforts are proposed for frameworks with IoT based applications in which honey pot empowered interruption discovery part adds additional profundity to the guard. A keen attacker may realize that a straightforward or direct attack is probably not going to be powerful. Subsequently, he/she may attempt to deceive the framework by stirring up his/her activities. Accepting that the attacker is additionally mindful of the protector's tricky barrier methodologies, with a specific end goal to boost the possibility of trading off the objectives, this aggressor additionally camouflages his/her activities. At the point when the attacker is dynamic, he/she can dispatch either a suspicious attack, which is one of the regular assault designs, prone to be perceived by the interruption identification framework; or an (apparently) typical action, which is in truth a very much camouflaged assault.

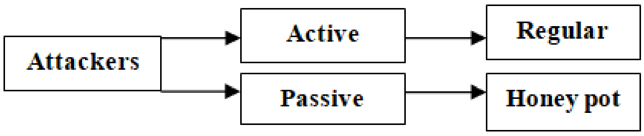

Figure 2: Description of the system

Despite what might be expected, when the attacker is latent, he/she can dispatch an ordinary movement as a standard client, which is totally safe; or a suspicious action which is to test the framework. Testing is an endeavor to take in the idea of the framework as concentrated in related models of trickiness, e.g., to put it plainly, paying little heed to types (i.e., dynamic or latent), the aggressor's activities can be identified as either ordinary or suspicious. The protector needs to permit just the correct clients to get to standard frameworks and trap those with malevolent purposes. The one-shot assault and protection diversion catches one experience between the protector and an obscure aggressor. Over the long haul, the protector faces countless experiences freely. The circumstance can be demonstrated as limitlessly numerous reiterations of the one-shot amusement after some time, i.e., a rehashed adaptation of the assault and resistance diversion. In game hypothesis, this has a place with the class of diversions known as multi-arrange recreations with watched activities and fragmented data.

A. Honey Pot enabled Networks

To provide protection against potential attacks, multi-layer security measures are proposed for systems with IoT-based applications [4]. One such structure is recorded in, where an interruption recognition framework (IDS) dissects the approaching traffic flow as indicated by some predefined contents. Suspicious traffic will be rerouted to the honey pots to be logged and additionally examined. [5] Whatever remains of the traffics are coordinated to the general frameworks among which are the aggressor's objectives.

B. Attackers and Defenders

There are attackers who plan to trade off these powerless focuses for their own pick up. A savvy aggressor may realize that a basic or direct assault is probably not going to be compelling. Consequently, he/she may endeavor to cheat the framework by stirring up his/her activities. That is, a portion of the circumstances he/she can act stealthily by claiming to be an innocuous client who does typical exercises and sits tight for the following opportunity. Accepting that the attacker is additionally mindful of the safeguard's misleading barrier techniques, so as to augment the possibility of trading off the objectives, this assailant additionally camouflages his/her activities. At the point when the aggressor is dynamic, he/she can dispatch either a suspicious assault, which is one of the regular attack designs, prone to be perceived by the interruption discovery framework; or an (apparently) "ordinary" action, which is in certainty a very much camouflaged assault.

3. System Implementation

The detailed implementation of the proposed system includes module description and algorithm description. The modules of this system are collect data, find abnormal events, detect active and passive user and honey pot.

A. Data Collection

This module loads the datasets that are used in this project work. This module selects data from the drive storage to load into database. Then load the data into database for analysis and Pre process the data to remove the irrelevant record from the data then view preprocessed data for acknowledgement.

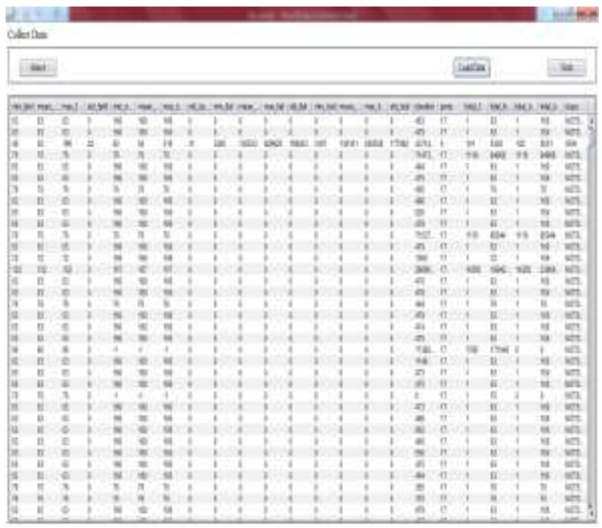

Figure 3: Collecting Data

B. Finding abnormal events

Get preprocessed data to find out the abnormal events from the whole data records. Then analyze user activities using their port address. Find out the abnormal events from the normal events. Then view collected abnormal data.

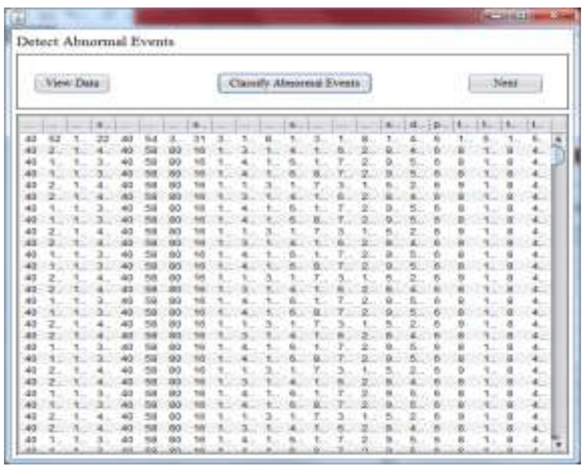

Figure 4: Detecting abnormal events

International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2016): 79.57 | Impact Factor (2017): 7.296

C. Detect active and passive user

This module uses game theory to classify passive users. Here gather information about abnormal events and the original data. Classify the active user and the passive user with their behavior analysis. Then view both active user data and passive user data.

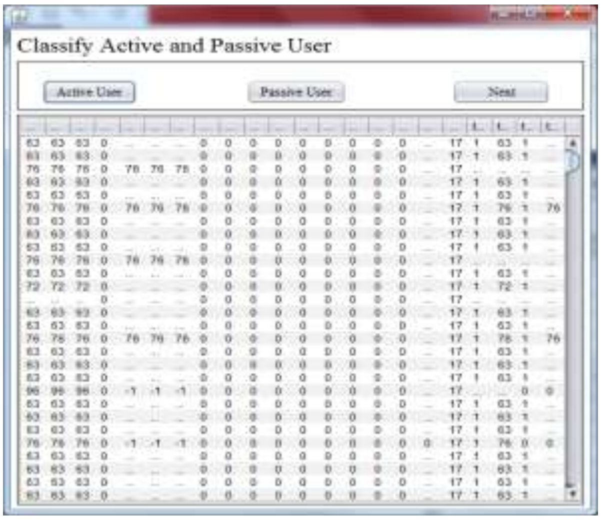

Figure 5: Classifying active and passive users

D. Honeypot

Get report of active and passive user. The active users are, then directed to the regular system. The passive users are redirected to honey pot. Then view honey pot user for acknowledgment. After that store passive attacker port address to future analysis.

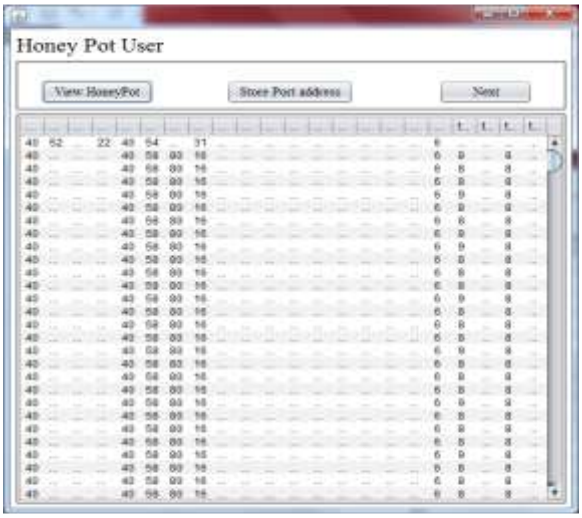

Figure 6: Honeypot

4. Implementation Results and Discussion

The system is implemented in Java and net beans IDE. In the existing system data offloading is done. Figure 7 shows the data offloading data transmission in the existing system. The data is loaded and is then spitted according to nodes file size. Then the data is transmitted into different nodes according to the protocols. Then it is allocated in to different servers. Then it is spitted based on keywords. There can be chances of attacks in the network. It can be detected but cannot be prevented.

Figure 7: Data Offloading In the existing system

In the proposed system the dataset is loaded and the data is preprocessed. Figure 8 shows the active and passive user reports. Then abnormal events are classified. Then active and passive users are identified and calculated. Then active users are moved to the regular system and passive users are moved to honey pot. Then the addresses are stored in the port.

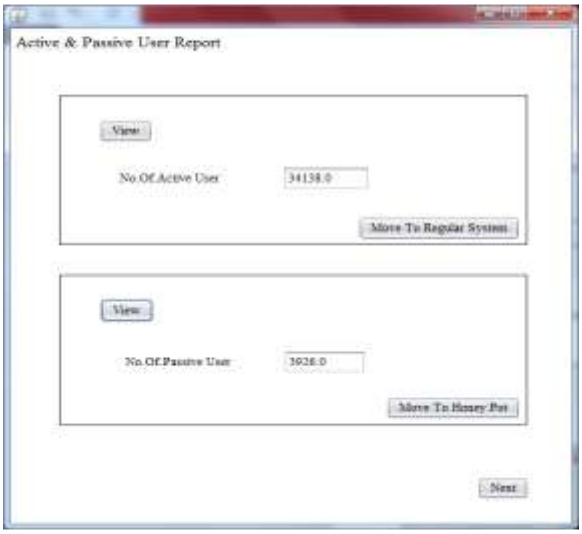

Figure 8: Active and passive user reports

5. Conclusion

In this paper the deceptive attacks and anomaly detection is done using honey pot enabled network. The active and passive users in the network are identified. The passive users are directed to the honey pot and attacks are effectively prevented. The problem is modeled as a Bayesian game of incomplete information. The game was further extended to account for the presence of false positives and false negatives in the defender's intrusion detection system. As a future work several features can be added to this to prevent attacks effectively and can be implemented in the emerging networks.

Reference

[1] D. C. Daniel and K. L. Herbig, Strategic Military Deception. New York: Pergamon Press, 1982.
[2] C. Kwon, W. Li, and I. Hwang, "Security analysis for cyber-physical systems against stealthy deception

attacks," in Proc. American Control Conference, Jun. 2013, pp. 3350–3355

[3] R. Mehresh and S. Upadhyaya, "A deception framework for survivability against next generation cyber attacks," in Proc. International Conference on Security and Management (SAM'12), Jul. 2012

[4] T. E. Carroll and D. Grosu, "A game theoretic investigation of deception in network security," Security Comm. Networks, vol. 4, no. 10, pp. 1162–1172, 2011.

[5] J. Lin, P. Liu, and J. Jing, "Using signaling games to model the multi- step attack-defense scenarios on confidentiality," in Proc. Decision and Game Theory for Security (GameSec). Springer-Verlag, 2012, pp. 118–137