International Journal of Engineering and Techniques - Volume 3 Issue 3, May-June 2017

RESEARCH ARTICLE OPEN ACCESS

A Survey on Deceptive Attack and Defense Game in Honeypot-Enabled Networks for IOT

K.Thenmozhi[1], E.Dilip kumar[2]
[1]PG Student, [2]Associate Professor
[1, 2,] Department of MCA, Dhanalakshmi Srinivasan College of Engineering and Technology

Abstract:

Nowadays internet is growing faster and the number of people using the internet is also growing. Hence, global communication using internet is getting more important every day. On the other hand, attacks on internet are also increasing gradually. Many of the intrusion detection system and firewall are protected the network intrusion but it is not fully protect the current network attacks. Honeypots have been considered as one of the methods to ensure security for networks in the Internet of Things (IoT) realm. This paper presents defend against attackers in honeypot enabled networks and to monitor the attacker's behavior. In this paper we are taking the normal patterns to find if an attacker comes into the system and behaves an attack. If the pattern mismatches then we find out it is an attacker and it is moved to honeypot system. This paper helps us to create a well secured system and also to monitor the attacker suspicious or not.

Keywords—**Data mining, Securities, Wiener process, Heston's Model, Brownian Motion, Clustering , Neural Networks**

I. INTRODUCTION

Due to rapid growth of internet technology, people easily retrieve their information and quickly transfer messages. This also strengthens the need for protection against cyber-attacks, as virtually any devices with a wireless connection could be vulnerable to malicious hacking attempts. Honeypots as a mechanism of deception to add an extra layer of defense to the IoT network [1].The Internet of things (IoT) is the inter-networking of physical devices, vehicles, buildings and other items - embedded with electronics, software, sensors, actuators and network connectivity that enable these objects to collect and exchange data [2] [3] [4].Internet of Things is the basis for a lot of services that depend on its accessibility and consistent operations. The IoT will serve as a conceptual background for future "smart" systems and applications such as the smart grid, smart building and home automation systems, smart healthcare and medical systems, environmental monitoring systems, and critical industrial control systems such as supervisory control and data acquisition (SCADA) systems. Meanwhile, honeypot based deception mechanism has been considered as one of the methods to ensure security for modern networks in the Internet of Things (IoT).Wikipedia [Wikip 05] defines a Honeypot as: "a trap set to detect or deflect attempts at unauthorized use of information systems." Honeypots 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 countermeasures [5].By deploying honeypots in the system, the defender hopes to lure attackers into these targets, which allows him/her to detect, study and intercept these attacks. The purpose of a Honeypot is to detect and learn from attacks and use that information to improve security. Attackers are also constantly trying to avoid being detected with stealthy deceptive attacks. Hidden attacks may appear normal and are hard to recognize. The defender, equipped with an intrusion detection system framework using honeypots, needs to carefully sieve out suspicious traffic from normal traffic, which might incur high costs if honey pots are used excessively, at the same time, doing so without knowledge of whether the incoming users are malicious or not adds to the defender's difficulties. The attacker may try to deceive the defender by employing different types of attacks ranging from a suspicious to a seemingly normal activity, while the defender in turn can make use of honeypots as a tool of deception to trap attackers. In this we are taking the normal patterns to find if an attacker comes into the system and behaves an attack. If the pattern mismatches then we find out it is an attacker and it is moved to honeypot systems.

II. LITERATURE SURVEY

Design and deployment of honeypots have also been extensively documented [6] and carry a rich literature. Garg et al. [7] studied the problem of allocating N real systems and honeypots within a block of IP addresses, which resulted in uniformly random strategies for both defender and attacker. P`ıbil et al. [8] proposed a honeypot selection game to examine the scenario where an attacker chooses which systems to attack, each of which has different values of importance. Carroll et al. [9] used a signaling game to investigate the interaction between defender and attacker. Many existing schemes available in the literature are used to find out the attackers and not their behaviors. The attacker is finding out using the behavioral changes between the normal user and the mismatched user. After the attacker is found then it is blocked to the account. Most of the aforementioned work focused on the deceptive strategies of defenders, specifically how to minimize the probability of having a real system under attack. Meanwhile, attackers often were modeled to have fixed, straightforward actions such as generic attacks, probes, and withdraw. Attacker's natures and their deceptive actions are ignored. In our work, we will look at deceptive strategies from both sides simultaneously and study the game outcomes in both short and long terms. In this, there is a drawback occurs (i.e.) when we block a malicious user to the authorized account we cannot find the behavior of the user.

Disadvantages of Existing System

- Behavioral Changes Not Monitored
- Systems are not secure for Passive Attackers
- Suspicious Users Activities are not Monitored
- Result into an Unsecured System

III. PROPOSED SYSTEM

Modern smart devices are also running some critical operations such as data collection and real-time monitoring, which makes them attractive targets to malicious attackers. In our proposed system we want to find out the attacker and its behavior. If we want to find the behavioral pattern for a malicious user means, the users who are all entering into the account gets monitored and when the behavioral pattern of the logged in user matches with the malicious user's pattern then we also monitor this user as malicious user's behavior. To provide protection against potential attacks, multi-layer security measures are proposed for systems with IoT-based applications in which honeypot-enabled intrusion detection component adds extra depth to the defense [10]. One such framework is documented in, where an intrusion detection system (IDS) analyzes the incoming traffic flow according to some predefined scripts. Suspicious traffic will be rerouted to the honeypots to be logged and further analyzed. The rest of the traffics are directed to the regular systems among which are the attacker's targets. Here, our task will be to model and analyze the attack and defense actions taking place between the IDS and an attacker, the analysis results of which could be helpful in implementing strategic measures for the IDS. The overall System Architecture is shown in the figure Fig 1.

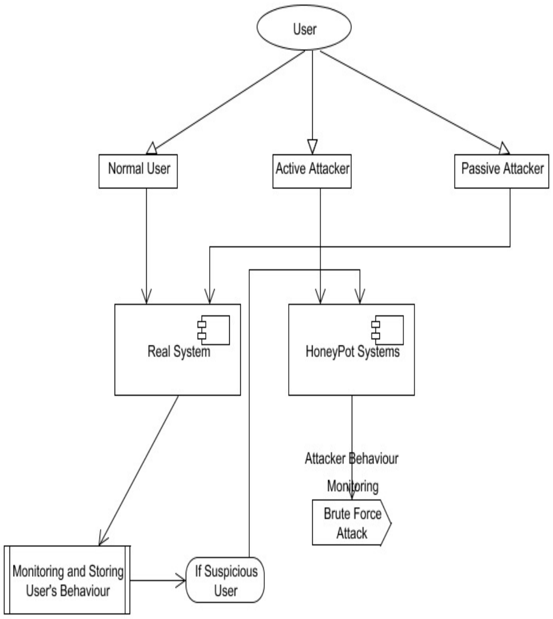


Fig.1 System Architecture

The System Modules Classifications are :

A. Normal Users Authentication and Behavior
B. Dashboard Controls of Users
C. Honeypot Networks
D. Passive and Suspicious Users to Honeypot

A. Normal Users Authentication and Behavior:

In this, the user will authenticate into the system and then the user will control the system and its operations. If this user is a normal user means its behaviors are stored it to normal patterns list. If the behaviors of a user are stored in normal pattern means, the user does not cross the limits of a normal user.

B. Dashboard Controls of Users:

The user is an attacker or not, if the user enters into the system means the dashboard control will be displayed the user. If the user is normal user not attacker means the system will be safe. Instead, if the user is attacker means then it will destroy the system. Because of this reason, honey pot networks are used. The user behavior is mismatched with the normal patterns user's list means then the admin will redirect it to honeypot network.

C. Honeypot Networks:

If the user is entering into the honeypot system means the user will feel it as the real system but the functionalities will be changing because of the users behavior must not reflect the system. When the attacker is active, he/she can launch either a "suspicious" attack, which is one of the common attack patterns, likely to be recognized by the intrusion detection system; or a (seemingly) "normal" activity, which is in fact a well-disguised attack. On the contrary, when the attacker is passive, he/she can launch a "normal" activity as a regular user, which is completely harmless;

or a “suspicious” activity which is to probe the system. Probing is an attempt to learn the nature of the system as studied in related models of deception.

D. Passive and Suspicious Users to Honeypot:

When the attacker is passive, its behaviors will noted as a suspicious user and the patterns are not matched means it will declare it as the attacker and the users actions will not reflect the system and the system will be secured. But, if the suspicious user activity is matched with the normal pattern means mistake it has been taken as a suspicious user and the user’s actions will continue its operations.

Advantages of Proposed System

- Behavioral Changes are Monitored
- Suspicious Users Activities are Monitored
- Systems are secure for Passive Attackers
- Attackers methods and tools have been releaved

IV. RESULT

The proposed system is implemented in java. First we need to register with name, mobile number and password as shown in the following figure Fig.2. After registration login with the username and password that is given during the registration.

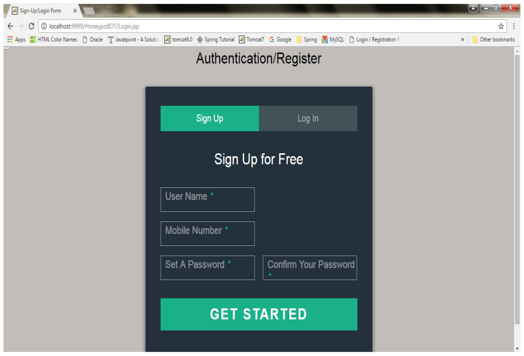


Fig.2 Authentication/Register

Then the User Control page will be displayed after login as shown in the following figure Fig.3.

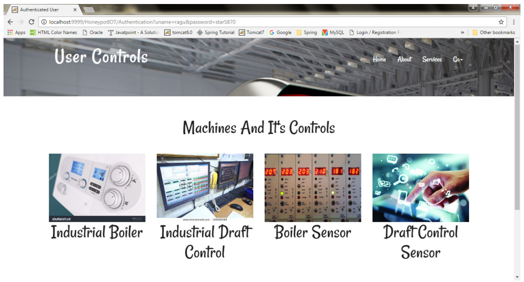


Fig.3 User Control page

The user has the control to change temperature, oxygen, carbon dioxide, pressure, carbon monoxide and the firing rate needed to the IoT machines within dashboard of controls as shown in Fig.4.

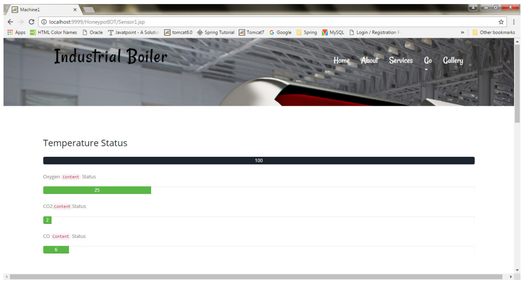


Fig.4 Boiler Control

The normal user are also has some restriction to change the controls as shown in the Figure Fig.5.

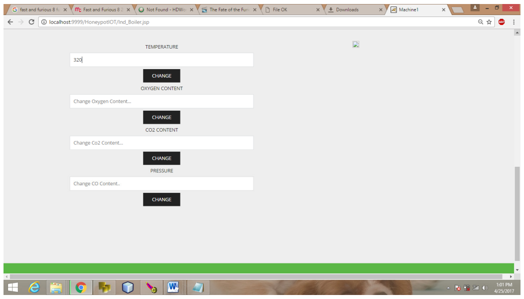
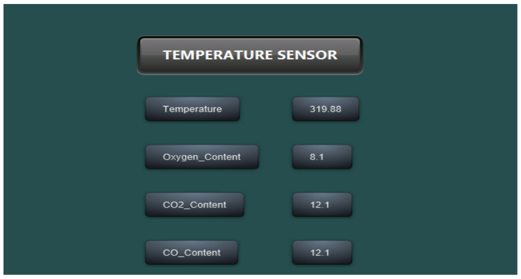


Fig.5 Change Control

When a normal user changes any controls in the front end means it also reflects in the back end as follows in figure Fig.6.

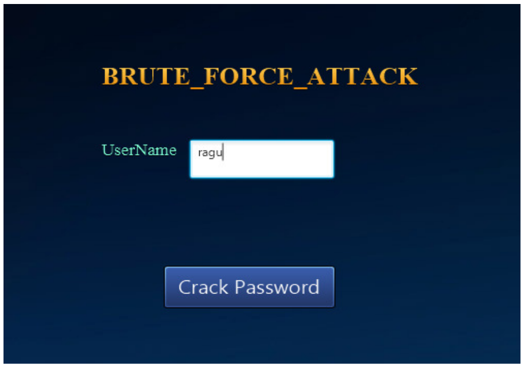


TEMPERATURE SENSOR

Temperature	319.88
Oxygen_Content	8.1
CO2_Content	12.1
CO_Content	12.1

Fig.6 Temperature Sensor

The active attacker can login the system using brute force algorithm as it cracks the password and allow him/his into the honeypot system as shown in the Figure Fig.7.

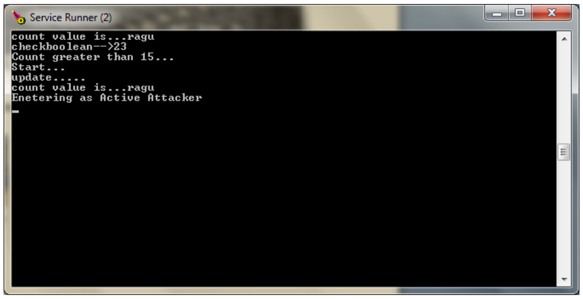


BRUTE_FORCE_ATTACK

UserName: ragu

Fig.7 Brute Force Attack

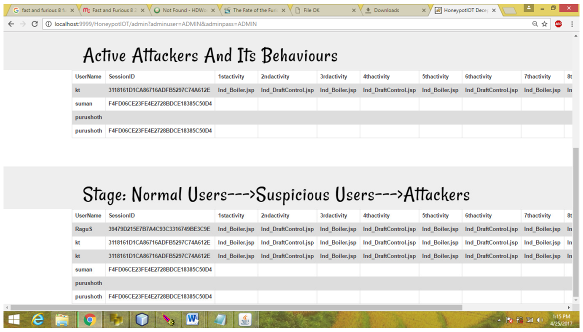
Whenever a change in the machine control by the active attacker it will not reflect back end data and the attacker is continuously monitoring by the admin.



```
count value is...ragu
checkboolean-->23
Count greater than 15...
Start...
update.....
count value is...ragu
Enetering as Active Attacker
```

Fig.8 Active Attacker login

Similarly the passive attacker can enter as normal user then turns to suspicious user and heavy monitoring has been taken place to them and their behavioral activities has been stored in the honeypot system as shown in the following figure Fig.9.



Active Attackers And Its Behaviours

UserName	SessionID	1stactivity	2ndactivity	3rdactivity	4thactivity	5thactivity	6thactivity	7thactivity	8t
kt	3118161D1CA86716ADFB5297C74A612E	Ind_Boiler.jsp	Ind_DraftControl.jsp	Ind_Boiler.jsp	Ind_DraftControl.jsp	Ind_Boiler.jsp	Ind_DraftControl.jsp	Ind_Boiler.jsp	In
suman	F4FD06CE23FE4E2728BDCE18385C50D4								
purushoth									
purushoth	F4FD06CE23FE4E2728BDCE18385C50D4								

Stage: Normal Users--->Suspicious Users--->Attackers

UserName	SessionID	1stactivity	2ndactivity	3rdactivity	4thactivity	5thactivity	6thactivity	7thactivity	8t
RaguS	39479D215E7B7A4C93C3316749BE3C9E	Ind_Boiler.jsp	Ind_DraftControl.jsp	Ind_Boiler.jsp	Ind_DraftControl.jsp	Ind_Boiler.jsp	Ind_DraftControl.jsp	Ind_Boiler.jsp	In
kt	3118161D1CA86716ADFB5297C74A612E	Ind_Boiler.jsp	Ind_DraftControl.jsp	Ind_Boiler.jsp	Ind_DraftControl.jsp	Ind_Boiler.jsp	Ind_DraftControl.jsp	Ind_Boiler.jsp	In
kt	3118161D1CA86716ADFB5297C74A612E	Ind_Boiler.jsp	Ind_DraftControl.jsp	Ind_Boiler.jsp	Ind_DraftControl.jsp	Ind_Boiler.jsp	Ind_DraftControl.jsp	Ind_Boiler.jsp	In
suman	F4FD06CE23FE4E2728BDCE18385C50D4								
purushoth									
purushoth	F4FD06CE23FE4E2728BDCE18385C50D4								

Fig.9 Admin View Page

Thus the activities of attackers has been stored and their deception of tool used to attack has been found .The honeypot system provide a secure system to all the attackers.

V. CONCLUSION AND FUTURE ENHANCEMENT

In this paper, we proposed a honeypot based IOT system which is used for the security of a system from active and passive attackers. This system helps us to monitor the behavior activities of both active and passive attackers. We show the active attacker using brute force attack and passive attacker using behavior pattern. Honeypot is also very useful for future threats to keep track of new technology attacks.We also use the attacker deception tool as a reference to create a better system in future.

REFERENCE

[1] W. Zhang and B. Qu, “Security architecture of the Internet of Things oriented to perceptual layer,” Int. J. Comput. Consum. Control, vol. 2, no. 2, pp. 37–45, 2013.

[2] Brown, Eric (13 September 2016). "Who Needs the Internet of Things?” Linux.com. Retrieved 23 October 2016.

[3] Brown, Eric (20 September 2016). "21 Open Source Projects for IoT". Linux.com. Retrieved 23 October 2016.

[4] "Internet of Things Global Standards Initiative". ITU. Retrieved 26 June 2015.

[5] The Honeynet Project, Know Your Enemy: Learning about Security Threats, 2nd ed. Addison-Wesley Professional, 2004.
[6] X. Liang and Y. Xiao, "Game theory for network security," IEEE Commun. Surveys Tuts., vol. 15, no. 1, pp. 472–486, 2013.
[7] N. Garg and D. Grosu, "Deception in honeynets: A game-theoretic analysis," in Proc. IEEE Workshop on Information Assurance, 2007, pp. 107–113.
[8] R. P`ıbil, V. Lis´y, C. Kiekintveld, B. Boˇsansk´y, and M. Pˇechouˇcek, "Game theoretic model of strategic honeypot selection in computer networks," in Proc. Decision and Game Theory for Security (GameSec). Springer-Verlag, 2012, pp. 201–220.
[9] 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.
[10] W. Hurst and C. Dobbins, "Guest editorial special issue on: Big data analytics in intelligent systems," Journal of Computer Sciences and Applications, vol. 3, no. 3A, pp. 1–9, 2015.
[11] C. Scott. (2014) Designing and implementing a honeypot for a SCADA network. [Online]. Available: http://www.sans.org/readingroom/whitepapers/detection/designing-implementing-honeypot-scadanetwork-35252
[12] J. Markert and M. Massoth, "Honeypot framework for wireless sensor networks," in Proc. Intl. Conf. Advances in Mobile Computing & Multimedia, Dec 2013, pp. 217:217–217:223.