ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 8, August 2017

Keen Honeypot based E-Commerce Security Model

B.V.Rama Krishna[1], B. Sushma[2]

Associate Professor, Dept. of CSE, Vardhaman Engineering College, Hyderabad, Telangana, India [1]

M.Tech (CSE) Student, Dept. of CSE, Vardhaman Engineering College, Hyderabad, Telangana, India[2]

ABSTRACT: E-Commerce playing the vital role in daily money transaction governance. Transmitting money over digital networks promotes cash-less transaction. This is becoming as a common way to fund transfers. B2B, B2C and C2C domains perform huge amount of transactions daily. It is necessary to provide security to these e-commerce portals. In this paper an intelligent honey-pot (keen-Honeypot) based model proposed by authors to secure e-commerce transactions from intruders and attacks. These k-Honey Pots support self analysis and decision support to track activities of hackers. They help in self governance and shielding E-Commerce portals with an inbuilt data mining services support.

KEYWORDS: k-Honeypot; layered; attackers; intruders; Honeypots; E-comerce

I. INTRODUCTION

Current E-commerce infrastructure is facing new challenges from increased threats and attacks. Firewalls, VPNs and Intrusion Detecting Systems are the only dependable services since long run [1]. These systems suffer from some weaknesses and are limited capabilities to handle attacks. Honeypot [1][2] is a special system which represents as a decoy for vulnerable systems to track activities of attackers. Two kinds of Honeypots available they are Production and Research Honeypot systems. Table 1 shows the services offered by them. The researching Honeypots currently available are with limited scope and to be audited by authorities who govern them periodically. The more they exposed to hackers more chance to organization security breaches.

TABLE 1
HONEYPOT SYSTEM CLASSES

Class	Services Offered
Production(Pure)	Log Intrusions, Vulnerable areas and Security Breaches detection using minimal data patterns
Research	Limited detection on attacking patterns, Intrusion behaviour and Policy violations, Complex large data capturing.

Honeypots can scan and detect any connection that is sent to it most data it collects represents unauthorized activities over network [3]. A group of Honeypots connected to form Honey Net which maintains a combination of Low-Interacting, High-Interacting and pure Honeypots [6]. Honey Nets [4] are widely used in e-commerce organizations to trap and track intruder activities more efficiently. Service Specific Honeypots [5] introduced new approach to construct a Honeypot based on the services of the network where they are implanted. A novel approach introduced to generate alerts to authenticated users about their password hackings by using Honey word mechanisms [7] but still Honeypots suffer from lack of self analysis and decision making features.

Online banking systems suffer from many security threats daily [8]. The Honey nets established over organizations open networks performance need to be increased in modern digital media. New cyber attacks influencing security credentials [9] of customers accessing services in E-commerce zones. Secured Electronic Transaction (SET) and Privacy Enhancing Transaction (PET) are widely used encryption oriented services in E-Commerce [10] provide security for online fund transfers which are highly sensitive to attacks. The Honeypot nets established over commerce based networks gathers the information about attacker behaviour.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 8, August 2017

In section 2 authors proposed E-commerce Keen-Honeypot layer based architecture. In Section 3 organization of the proposed system explained. A comparative view projected in Section 4 followed by Conclusion and Future work.

II. HONEY POT SERVER ARCHITECTURE

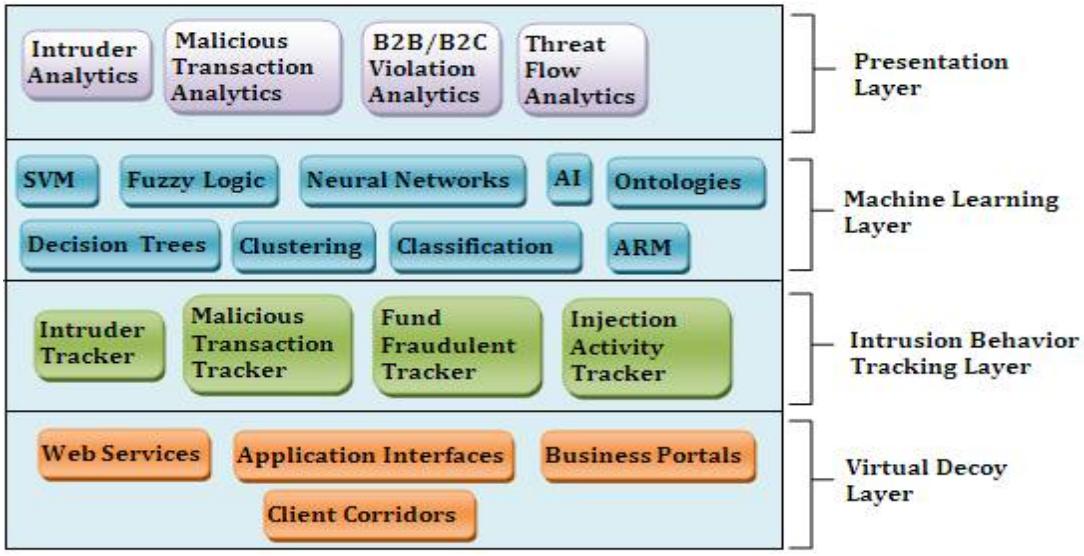

Fig. 1 E-Commerce Keen Honey Pot Layered Architecture

A. Virtual Decoy Layer

The role of this layer is to behave like a virtual real-time platform for business and customer transaction services. A decoy platform constructed to attract Hackers, Intruders and Hi-Jacks. It represents all the services of E-Commerce like web services, application interfaces, business portals and client corridors (e-shopping, e-markets and apps). Simply acts as a decoy of e-commerce server. The layer is a Magnet-Zone where hackers, Intruders can be easily hooked without their awareness.

B. Intrusion Behavior Tracking Layer

The in-built modules of this silently track necessary information while intruder performing his activities in virtual decoy layer. Separate modules handle the information about Hacker behavior such as listed below in Table 2.

TABLE 2
INTRUSION BEHAVIOR STATISTICS

Intrusion Type	**Behavior Statistics**
Intruders	Unauthorized access, Credential Stealing, Unauthorized Transaction Inspection and Activities(Masquerader/Misfeasor/Clandestine)
Malicious Transaction	Transaction activities violating B2B and B2C rules
Fund Fraudulent	e-Purse hacking, Fund Diverting, security breaches and Unauthorized access
Injection Activity	Malicious code injections, service blocking, unauthorized regulation of e-commerce activities

The layer designed to capture information from wide range of Intruder activities. The individual statistics converted into adoptable form for DM-Tool layer which is the upper layer.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 8, August 2017

C. Machine Learning Layer

The most important layer in this model with Data Mining interfaces to perform Machine Learning activities over Intrusion statistics. A large set of knowledge engineering tools interfaced to this layer to perform machine learning activities as follows:

- SVM {Permutation tests, classification and regression analysis}
- Fuzzy Logic {Association ships, Logical deductions and decision support}
- Neural Networks {Pattern recognition, Cross-Validations, functional dependencies and complex relationships estimation}
- AI & Ontologies {hierarchical relations, tagging, annotations, Mixed variable estimation and deep learning}
- Decision Trees {Decision making on rule based}
- Clustering {grouping of items based on statistical measures}
- Classification {Identifies the groups using supervised learning schemes}
- ARM {performs association rule mining over data to generate association rules as well as to identify frequent item sets}

D. Presentation Layer

The high end layer which interact with administrators and organization authorities of business servers and e-commerce servers. This layer provides visualization of machine learning statistics of Intruder behavior analysis. Thus system analysts can acquire knowledge on current trends of attacker activities, also data mining layer assists with decision support system to better handle the security issues over E-commerce networks.

III. ORGANIZATION OF PROPOSED SYSTEM

The proposed Keen Honeypot system organization was shown in the Figure 2. The Keen Honeypot System for E-commerce enterprise network placed between E-commerce central server and Wi-Fi gateway router. The major components of architecture are as follows

Login Server: Manages the client accounts and private credentials and hooked up with K-Honeypot server to transfer virtual view of the server.

B2B Server: Provides portals and services for B2B E-commerce transactions. Regulated using set of B2B policies. Support virtual transmission link with K-Honeypot server.

B2C Server: Provides platform for B2C services governed by E-commerce server. Maintain a transmission link with K-Honeypot server to manage the decoy of B2B server to trap hackers.

C2C Server: Supports services of E-commerce related to C2C domains. Maintain virtual transmission link with Honeypot server to manage virtual C2C environment to attract intruders.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 8, August 2017

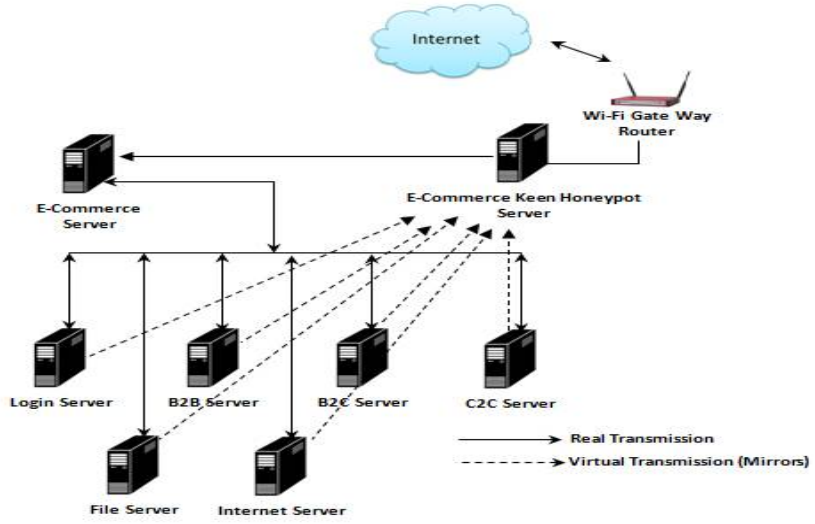

Fig. 2 E-Commerce Honey Pot System Architecture

E-Commerce Server: The organizational private server manages all the transactions, e-commerce services under the policies and regulations issued by authorities of organization. The server supported with secured encrypted File Server and an Internet Server.

Mirrors: These are virtual transmission lines transfer real-time transaction activities snapshots to Honeypot Server from which it constructs decoys of e-commerce servers. Hackers and attackers attracted by these mirrors.

E-Commerce Keen Honeypot Server: Designed to attract attackers and silently track their attacking behavior. They have ability to divert them from sensitive zones of organizational network. Intelligent decision making support assisted with data mining tools enables these Honeypot systems to apply security policies, privileges and shields to services, files and applications related to e-commerce server. The proposed keen Honeypot system autonomously performs analysis over collected information using knowledge engineering tools. They provide better information with valuable analysis summaries to organization.

IV. KEEN-HONEYPOT VS. HONEYPOT

The Keen-Honeypot extended its ability from simple tracking services to advanced decision making services. Ordinary Honeypot perform a spy over attacker's behavior and Intrusion activities whereas Keen-Honeypot integrated with Data Mining services to perform knowledge engineering on captured data. Table 3 gives the insight view about variation among both Honeypots.

TABLE 3
KEEN-HONEYPOT VS. HONEYPOT

Keen-Honeypot	Honeypot
Tracks behavior of attackers	Tracks behavior of attackers
Collects information about • Log details • Credential breaches • Security breach activities • Intruder activities • Hackers behavior	Collects information about • Log details • Credential breaches • Security breach activities • Intruder activities • Hackers behavior

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 8, August 2017

Automatic analysis with Data Mining tools	Manual analysis of Intrusion statistics
Policies adjustments using Decision Support System	Manual adjustments of policies
More refined knowledge extraction using knowledge engineering techniques	Highly qualified professionals need to perform analysis on the site.
Maintains trends of data about attacks in pre-processed format.	Maintains only limited period of data in raw format only.
Design time complexity is high but durability and performance is versatile	Design time complexity is low but performance is low. Durability is inconsistent.
High research activities with machine learning tools	Medium research activities with in-built static modules.

The proposed layered architecture needs an interlacing between Honeypot system and Data Mining system.

V. CONCLUSION

The proposed architecture Keen-Honeypot by authors reduces the human expert's consistent analysis over Honeypot data. It helps enterprises to overcome the demand of employing large amount of highly skilled network security professionals to monitor E-commerce server day to day. The scope and efficiency of intelligent decision making capabilities of proposed Honeypot server depends on the employed machine learning mechanisms by Data Mining engine. In future a real-time Keen-Honeypot Server implementation with the integration of a third party Data Mining tool is the further work of this paper. Also a direction of research going on to develop self analysis and policy creation mechanism which suggests new policies to defense more effectively attacks on E-Commerce systems in enterprises.

VI. CONCLUSION AND FUTURE WORK

The simulation results showed that the proposed algorithm performs better with the total transmission energy metric than the maximum number of hops metric. The proposed algorithm provides energy efficient path for data transmission and maximizes the lifetime of entire network. As the performance of the proposed algorithm is analyzed between two metrics in future with some modifications in design considerations the performance of the proposed algorithm can be compared with other energy efficient algorithm. We have used very small network of 5 nodes, as number of nodes increases the complexity will increase. We can increase the number of nodes and analyze the performance.

REFERENCES

1. C. Sandeep, "Banking Security using Honeypot", IJSIA, Vol. 5, No. 1, pp: 31-38, 2011.
2. V. Dhamankar et. al., "Overview of Honeypot Security System for E-Banking", UARJ, Issue-1, Vol.1, ISSN: 2278-1129, 2012. pp. 98-102, 2012.
3. A. Chandra, "HONEYOTS: A NEW MECHANISM FOR NETWORK SECURITY"," PPAE-Journal, ISSN: 2230-8547, Vol.4, Issue-1, pp.211-217, 2013.
4. S. Deepa Lakshmi et. al., "Network Security Enhancement through Honeypot based Systems", IJET, ISSN: 0975-4024, Vol.7, No.1, Febraury-2015.
5. S. Narote et. al., "Advanced Honeypot System for analyzing Network Security", ISSN: 2347-3215, pp: 65-70, Vol. 2, No. 4, April-2014.
6. N. Sonali et. al., "Honeypot Security System: An efficient approach of securing E-banking network", IRJMS, ISSN:245-8499, Vol.1, Issue-5, December-2015.
7. A. Gawali et. al., "Improving Security using Honey Word for online Banking Authentication System", IJAERD, ISSN:2348-6406, Vol. 3, Issue-10, October-2016.
8. D.Pandey et. al., "E-Commerce Transactions an Empirical Study", IJARCSSE, Vol. 4, Issue-3, March-2014.
9. B.N. Khandare, "Transaction Security for Internet E-Commerce Application", IJARCSSE, Vol.5, Issue-2, Febraury-2015.
10. Palak Gupta et. al., "E-Commerce Study of Privacy, Trust and Security from Consumers Perspective", IJCSMC, Vol.5, Issue-6, June-2016.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 8, August 2017

BIOGRAPHY

Mr. B.V. Rama Krishna currently working as Associate Professor in CSE department. He is pursuing Ph.D. (CSE) from Acharya Nagarjuna University. His areas of interest are Data Mining, Network Security, E-Commerce and Cloud Computing. He has 12 years of teaching experience and author of few journal publications.

Smt. B. Sushma currently pursuing her M.Tech (CSE) from JNTUH. Her areas of interest are Data Mining, Software Engineering, Networks and Security.