International Journal of Pure and Applied Mathematics
Volume 116 No. 10 2017, 197-200
ISSN: 1311-8080 (printed version); ISSN: 1314-3395 (on-line version)
url: http://www.ijpam.eu
Special Issue

ijpam.eu

DECOY METHOD ON VARIOUS ENVIRONMENTS – A SURVEY

S.Pothumani[1],Mrs.C.Anuradha[2]
[1,2]Assistant Professor, Department of CSE, BIST,BIHER,Bharath University
[1]pothumani@gmail.com,[2]anuradha.cse@bharathuniv.ac.in

Abstract: One of the biggest threats of internet communication system is data theft. To handle this number of technologies like encryption algorithms, firewall, and intrusion detection system are used. But this paper discusses a new technique named "decoy". This may be a document, traffic, network or system. Whenever data security is needed, this decoy provides efficient services. This can detect the insider attacker and end number of fogus information to the attacker and redirects the attacker from the original data. Some systems supports the decoy document is encrypted one. So the attacker believes the received document is the original data. So, the attacker easily redirects from the original data. This paper surveys different types of decoy methods in various environments.

1. Introduction

Recent days, one of the biggest growing technologies is information security. This is not only used by the organizations and also number of private users. There are lot of methods are available to prevent data from attackers. The existing systems provide number of solutions to data theft and to prevent the data from attack. But day by day[1-6], the attacks against computer networks are increased. A new technique named "decoy". This may be a document, traffic, network or system. Whenever data security is needed, this decoy provides efficient services[7-9]. This can detect the insider attacker and end number of fogus information to the attacker and redirects the attacker from the original data. Some systems supports the decoy document is encrypted one. So the attacker believes the received document is the original data

2. Related work

[1] Alleviating Internal Data Theft Attacks by Decoy Technology in Cloud

I.Sudha ,A.Kannaki , S.Jeevidha
The computing resources are used by various users with the help of cloud computing. They can retrieve and save their professional and private data. This new technology provides number of benefits and also some disadvantage. The biggest challenge in cloud computing is security of data. Insiders are the users who have the username and password. In security point of view, attackers are generally remote users. Some security systems do not secure data from data theft attackers. This paper proposes a new technique that decoy in cloud environment. In this system, large amount of decoy information provides to the attacker. So it provides security to the original data. By using the HMAC, the users can easily identified the document is decoy document or original data.

[11-15] Minimizing Internal Data Theft in Cloud Through Disinformation Attacks, P.Jyothi1 , R.Anuradha2 , Dr.Y.Vijayalata 3, International Journal of Advanced Research in Computer and Communication Engineering Vol. 2, Issue 9, September 2013
Cloud computing provide three types of services that are software as a service (SAAS), Platform as s service(PAAS) and Infrastructure as a service(IASS). The services are less expensive. One of the biggest challenge in cloud computing is data thefts attacks. This paper provides decoy documents to identify the insider data theft attacks. This paper builds a web based prototype. This explains the efficiency of decoy documents. Once a doubt on unauthorized access, this application simple provide the false information document using decoy technology. So this provides security from the insider attack. This paper provides good results against insider attack.

[4]Honeypots:concepts, approaches, and challenges, IyatitiMokubeArmstrong Atlantic State University, Savannah, GAMicheleAdamsArmstrong Atlantic State University, Savannah, GA, ACM-SE 45 Proceedings of the 45th annual southeast regional conference , Pages 321-326
Recent days, one of the biggest growing technologies is information security. This is not only used by the organizations and also number of private users. There are lot of methods are available to prevent data from attackers. This paper analyzes the concept of honeypots. Honeypot act as s security resource for the system. At the time of attack, it provides false document to the attacker. This

paper deals with various types of honeypot, the overall concept and method to implement the honeypot.

Bait and Snitch:

Defending Computer Systems with Decoys, Jonathan Voris, Jill Jermyn, Angelos D. Keromytis, and Salvatore J. Stolfo,ids.cs.columbia.edu/sites/default/files/ssi.pdf
The existing systems provide number of solutions to data theft and to prevent the data from attack. But day by day, the attacks against computer networks are increased. This paper implements a new technology named decoy technology which identify the attacker and also provide bogus information to the attacker. These attacks can be identified by monitoring this affected information. This system has the ability to identify the malicious activity like masquerade attacks and insider. This paper verifies the efficiency of decoy deployment for comprehensive security solution. This paper evaluates decoy technology in different situations. And also some efficient craft and distribute decoy tools are provided to form a network of sensors. These are used to identify attacks anywhere in particular network.
[6]Detecting Traffic Snooping in Tor Using Decoys, Sambuddho Chakravarty,Georgios Portokalidis,
, Michalis Polychronakis, , Angelos D. Keromytis
All the confidential data are encrypted and send to the anonymous communication network. But the attacker can attack the data when it travels from one end to other end. This paper deals with the decoy traffic to detect the interception of traffic in different proxy systems. This paper provides a new technology to inject the traffic that disclosers bait credentials for decoy services. The goal of this paper is that the eavesdroppers access decoy documents on servers under our control. This paper implements decoy traffic n Tor networks with the help of decoy IMAP and SMAP servers. In this system, ten diffident types of traffic interception identified. And this paper analysis detected incidents, implementation of decoy traffic and extension for identify HTTP session hijacking attacks.

Decoy Systems:

A New Player in Network Security and Computer Incident Response Kellep A. Charles, CISSP, International Journal of Digital Evidence Winter 2004, Volume 2, Issue 3
All over the world, lot of private and public organizations are connected and exchange the information. This provides good productivity, endless private services and faster communications. In this communication, High risk rate available. Some attackers may gain organizational data. The private and public organizations implements firewalls, router access to control list (ACLs), anti-viruses and intrusion detection systems. But these systems are failed to prevent data because of the various new hacking tools. A new technology is introduced in this paper named decoy systems. This is also named as deception system or honey pots or tar pits. This system is used to detect the unauthorized access on network and send fogus information.

3. Conclusion

This paper provides literature survey about different decoy technology papers. These survey papers analyzes various decoy methods like decoy as a document, decoy traffic, decoy system etc. This decoy method is not only identifying the attacker and also it sends false information to the attacker. Some systems supports the decoy document is encrypted one. So the attacker believes the received document is the original data. So, the attacker easily redirects from the original data. All the papers prove the decoy method is the best method to solve the threats of data security.

References

[1] Udayakumar R., Kaliyamurthie K.P., Khanaa, Thooyamani K.P., Data mining a boon: Predictive system for university topper women in academia, World Applied Sciences Journal, v-29, i-14, pp-86-90, 2014.
[2] Kaliyamurthie K.P., Parameswari D., Udayakumar R., QOS aware privacy preserving location monitoring in wireless sensor network, Indian Journal of Science and Technology, v-6, i-SUPPL5, pp-4648-4652, 2013.
[3] BrinthaRajakumari S., Nalini C., An efficient cost model for data storage with horizontal layout in the cloud, Indian Journal of Science and Technology, v-7, i-, pp-45-46, 2014.
[4] BrinthaRajakumari S., Nalini C., An efficient data mining dataset preparation using aggregation in relational database, Indian Journal of Science and Technology, v-7, i-, pp-44-46, 2014.
[5] Khanna V., Mohanta K., Saravanan T., Recovery of link quality degradation in wireless mesh networks, Indian Journal of Science and Technology, v-6, i-SUPPL.6, pp-4837-4843, 2013.
[6] Khanaa V., Thooyamani K.P., Udayakumar R., A secure and efficient authentication system for distributed wireless sensor network, World Applied Sciences Journal, v-29, i-14, pp-304-308, 2014.
[7] Udayakumar R., Khanaa V., Saravanan T., Saritha G., Retinal image analysis using curvelet transform and multistructure elements morphology by reconstruction,

Middle - East Journal of Scientific Research, v-16, i-12, pp-1781-1785, 2013.
[8] Khanaa V., Mohanta K., Saravanan. T., Performance analysis of FTTH using GEPON in direct and external modulation, Indian Journal of Science and Technology, v-6, i-SUPPL.6, pp-4848-4852, 2013.
[9] Kaliyamurthie K.P., Udayakumar R., Parameswari D., Mugunthan S.N., Highly secured online voting system over network, Indian Journal of Science and Technology, v-6, i-SUPPL.6, pp-4831-4836, 2013.
[10] Thooyamani K.P., Khanaa V., Udayakumar R., Efficiently measuring denial of service attacks using appropriate metrics, Middle - East Journal of Scientific Research, v-20, i-12, pp-2464-2470, 2014.
[11] R.Kalaiprasath, R.Elankavi, Dr.R.Udayakumar, Cloud Information Accountability (Cia) Framework Ensuring Accountability Of Data In Cloud And Security In End To End Process In Cloud Terminology, International Journal Of Civil Engineering And Technology (Ijciet) Volume 8, Issue 4, Pp. 376–385, April 2017.
[12] R.Elankavi, R.Kalaiprasath, Dr.R.Udayakumar, A fast clustering algorithm for high-dimensional data, International Journal Of Civil Engineering And Technology (Ijciet), Volume 8, Issue 5, Pp. 1220–1227, May 2017.
[13] R. Kalaiprasath, R. Elankavi and Dr. R. Udayakumar. Cloud. Security and Compliance - A Semantic Approach in End to End Security, International Journal Of Mechanical Engineering And Technology (Ijmet), Volume 8, Issue 5, pp-987-994, May 2017.
[14] ThooyamaniK.P., Khanaa V., Udayakumar R., Virtual instrumentation based process of agriculture by automation, Middle - East Journal of Scientific Research, v-20, i-12, pp-2604-2612, 2014.
[15] Udayakumar R., Thooyamani K.P., Khanaa, Random projection based data perturbation using geometric transformation, World Applied Sciences Journal, v-29, i-14, pp-19-24, 2014.
[16] Udayakumar R., Thooyamani K.P., Khanaa, Deploying site-to-site VPN connectivity: MPLS Vs IPSec, World Applied Sciences Journal, v-29, i-14, pp-6-10, 2014.