International Journal of Engineering & Technology, 7 (2.4) (2018) 187-189

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research Paper

A survey of intrusion detection techniques

Sharanya Chandran [1] *, K. Senthil Kumar [1]

[1] *Assistant Professor Department of Computer Science Engineering, SRM Institute of Science and Technology, Chennai, Tamil Nadu, India*

**Corresponding author E-mail: sharanya.chandran1@gmail.com*

Abstract

In today's world, the number of companies is increasing day by day that help end users to express opinion i.e. social media management, to watch news, payment applications, retail, ecommerce etc. There are large amount of forms, which take personal information's like username, password, social security number, credit card, debit card and account information. Thus the applications are vulnerable to security issues like phishing attacks, denial of service attacks, cross-site scripting attack and many more. This paper provides literature review of work done in these areas and their respective mitigations.

Keywords: *UDDI; Web Service; Clustering; Machine Learning; K-Nearest Neighbor.*

1. Phishing attack study

Phishing is a very critical security treat and the hackers are smart and adaptable. Number of websites being hacked day by day is increasing exponentially by using many different kinds of attack. One applications allow users to communicate with each other without much hassle and avoid travel for communication. The criminal activities [2] also increase because lot of websites has integrated with payment system and take lot of secure information like credit card information and social security number. The malware system gains control of victim and perform various Dos Attacks. Few of these attacks can be avoided by using a black list of URL's before rendering the response to client.

Network is a collection of computers where information exchange happens an d there is a main computer which acts like a agent controlling the tasks like load balancing and routing the packets at right locations. An intelligent network can be created by using a Secure Controlling agent which can perform the detection of Dos Attack and provide a defense mechanism. A Software Define Network Secure Controller [3] algorithm provides such a approach.

Control Systems are periodically triggered linearly triggered as well as event triggered systems. All the three systems are subjected to denial of service attacks. A two mode switching [4] control can be used in order to stabilize the event triggered control systems in the presence of Dos attacks.

In a Dos attack stabilization [5] of network is the most important priority. Mean Square is an important factor which studies the network performance. Dos attack is Monrovian in nature. Dual switch linear system can be used along with set of rules to provide regular feedback mechanism to controllers.

Scheduling of packets [6] and controlling the packet flow is most important communication constraint. In a cluster based mechanism there is special node which controls an area but is limited by transmission capability and will suffer from Dos attacks from external attacker. Linear quadratic criteria are used to determine the attacks for an external attacker and provide jammers to deny the service. A zero sum static game method creates different kinds of players namely designer and attacker and by means of Nash equilibrium the attackers are denied access to system.

The data consumption [7] analyzes is performed by Advanced metering infrastructure (AMI) which collects, stores and operates the data consumption rates. The channel between consumer and utilities are subjected to Dos arracks. A set of devices known as honey pots can be installed to detect and gather information about attackers and defenders and then provide suggestions for defenders to improve efficiency to mitigate attacks

In Software Defined Networking [8] software program can be used to control the network with the help of central control plane. The attacks can happen on central entity and data plane. Statics can be used to perform the scan of network and detect the attack and also the algorithm is bound to be light weight Cloud computing is the best technique used to perform services to many enterprises and government organizations. Security [9] is a challenge because most of the data is critical. Multi tenancy and elasticity provide more threats like energy denial of service attack. The subtle security issues an be avoided by managing the energy amoung various nodes in network.

For an intelligent transport system VANET is most important kind of strategy that is a technology trend. The data sent over the network is life crucial and the integrity of the information is very important. The resources and there energy levels gets exhausted due to fake identities created by spoofed IP addresses and bogus messages. The DDOS prevention [10] mechanism includes keeping the check of number of packets send over the network and controlling it

The syntactic signature is used in order uniquely identify any action or data. The malware creates a file which will be identical to original file.

2. Malware attack and prevention survey

The number of samples [11] that represent the malware increase exponentially. One alternative approach is to use behavior signature but is limited because of complexity and slowness if used in real time detection. An approach can be used which can nullify the

tracking of flow of data and create profile type of resources and make it scalable

The specifications about the malware [12] are needed to prevent number of false event detections using Behavior based analysis. Automatic detection of such specifications is very important and must be incorporated in behavior based malware detection. The algorithm can be created using a combination of graph mining and stochastic optimizer.

Two sets are created. One set corresponds to execution behavior of programs. The second set corresponds to behavior of malware. The mining is performed on the sets and output is generated. This output can be fed as an intelligent control into the malware detector [13] responsible for detecting malware variants.

There are generally two kinds of malware samples namely polymorphic and metamorphic [14]. The malwares are also huge. The current malware detection software's are based on signature and is not useful for new kinds of attacks. The detection method must take into consideration file characteristics, internal file properties and run time relationships.

The traffic volume in education is dramatically high [15]. Security information is critical for performing data mining on such large data set. Cloud Computing along with data mining can be used for marwaredetection and also data centers must be created for obtaining better resources

A set of instructions which can damage the network is called as malware [16]. Only known malicious programs can be detected using signature based method. Code polymorphism and metamorphism are included in new malwares which are hard to detect. Hence there must a marriage between data mining and machine learning to achieve the task.

3. Web security attacks and measures

The proliferation of Cloud Computing [17] (CC) is a internet based platform which reduces maintenance cost and also provides flexibility in terms of pay per use model. SQL Injection attacks runs queries on the database system that makes hackers to compromise security and integrity.

Web Usage [18] touches most of the parameters like life, economy and education. The hacking of the websites is also increasing on daily basis. An algorithm named online anomaly studies the behavior of web pages to detect malicious codes or pages. The algorithm makes use of parameters like feature selection, data mining, data analytics and statistical mining to detect the malicious behavior

PHP has been used since about 20 years in content based management system [19]. Word press has stack of over 25% market share of various websites and the web content is vulnerable for hacking. In traditional methods there is a white list of Ip addresses which are maintained. By using broad surface attack the system can be hacked using verbose blacklist. ZenId's makes use of an approach which finds the execution path of the user during a specific window and then report the intrusions that are performed.

The cybercrime has increased [20] exponentially with the evolution of internet. The categories of users, which are subjected to cybercrime, can be of two types namely personal and company users. The defense tool consists of firewall and intrusion detection module (IDM). Firewall allows the packets to pass based on certain set of conditions. IDM monitors the actions in the network. Bayesian classifier is used to classify the users into valid and invalid based on labeled data.

For an online social network [21], the validations must be performed properly on the user interface and backend. If these validations are not taken care then attackers can bypass the application. XSS and CSRF Attacks can be prevented by using encoding and unique token validations. Invariant Detector (IVD) detects the invariants based by learning and then blocks any request that try not to follow the pattern. IVD will be an additional cone to private frameworks for verification.

The web application security [22] is important factor which contributes to 60% of internet. The most common attack is Cross Site Scripting (XSS) attack and is one among top vulnerability of web application. The XSS occurs due to improper testing to secure coding related aspects. Intrusion Detection System is used for the purpose of XSS attack prevention.

The attacks on the web based applications are complex [23]. A single detection method is unsuitable for these cases. The combination of misuse and anomaly can be used for intruder identification. The events are captured in the web log file and it must be protected. The method finds the feature vectors in the HTTP request to find the abnormal behaviors and then model is created using k means clustering algorithm.

The unsafe vulnerability is the scripting attack on web pages known as cross site scripting (XSS) [24]. The intruder gains the access to system, gets authentication of user's web browser, and can perform session hijacking and malware induction. The most dangerous attacks are reflected and DOM based cross-site scripting attacks. The reflected and DOM based attacks are performed based on server side scripting Content Delivery Networks (CDN) [25] is responsible for redirecting web requests for from browsers to surrogate nodes. The CDN has two problems like security and resource allocation. Game theory can be used in CDN networks to prevent intrusion Many web based applications have been developed which spans in every sector like social, commercial, government and academic organizations. Cloud deployment [26] is the fast market and the cloud also is accessed through web based interfaces. SQL injection attacks are treat to applications and the attacks are detected based on user log analysis, machine learning or by using pattern matching. Supervised machine learning can detect attacks and be trained offline using a training data The web applications make use of signatures and profiles [27] The web server will check against the signatures and profiles to verify the validity of request and the requests are unpredictable.

Logs are intended for debugging purpose and tracking [28]. The log files maintain traces of events which contain user activity, applications and network traffic. Firewalls and Network devices can construct the malicious activities from log file and use this as a pattern to prevent attacks. Dictionary based classifier are used for normalizing log into columns and rows and then establish relationship between cells The online transactions volume is huge [29], In order to handle the data complexity multi-tiered architecture has to be used which contains database server or file server. The data access must be performed in a secure way to avoid miss use of data. Double Guard Intrusion will monitor both web server and the database server and prevent attacks.

Nation state actors [30] perform targeted attacks in an organized manner and pose a lot of criminal threats. Perimeter defenses are deployed to prevent the threats. The data is collected in log files and used for forensic investigation. Security analytics are used for proactive breach detection.

The digital patterns are detected [31] over the network by using Intrusion detection systems. Many hackers appear innocent from individual ids but malacious across end to end application. Complex end to end intrusions can be analyzed based on the logs. SAP Enterprise Detection takes data from multiple sources and then finally perform analysis.

Virtualization and data outsourcing [32] are two important factors of cloud computing. The two entities introduce lot of security risks. The patterns of the users in clustered using k means and then bisection between clusters is obtained forming hydrid distributed intrusion method. This method can detect known and unknown attacks. The initial cluster center is obtained in a stable fashion and after that for each iteration the cluster centers are changed.

4. Conclusion

The various types of attacks have been described like denial of service attack, phishing attack and then finally the intrusion detection methods. Each method has its own way for attack detection

and recovery. The main purpose of the survey is to find the methods and the approaches used so that the unified way can be determined in order to protect the web application from internal and external users attack in our future implementation.

References

[1] C. Yue and H. Wang, "BogusBiter: A transparent protection against phishing attacks," ACM Trans. Int. Technol., vol. 10, no. 2, pp. 1–31, May 2010.

[2] Tara Baniya ; Dipesh Gautam ; Yoohwan Kim,"Safeguarding Web Surfing with URL Blacklisting",Information Technology - New Generations (ITNG), 2015 12th International Conference,13-15 April 2015

[3] Song Wang ; Karina Gomez Chavez ; Sithamparanathan Kandeepan,"SECO: SDN sEcure COntroller algorithm for detecting and defending denial of service attacks",Information and Communication Technology (ICoIC7), 2017 5th International Conference,17-19 May 2017

[4] Tingting Cui ; Hao Yu ; Fei Hao,"Security control for linear systems subject to denial-of- service attacks",Control Conference (CCC), 2017 36th Chinese,26- 28 July 2017

[5] Jialei Hu; Chong Liu; Yang Song,"Switching control for networked control system with denial-of-service attacks",Control Conference (CCC), 2017 36th Chinese,26-28 July 201.

[6] Yinghong Zhao ; Xiao He ; Donghua Zhou,"Optimal joint control and triggering strategies against denial of service attacks: a zero-sum game",IET Control Theory & Applications (Volume: 11, Issue: 14, 9 22 2017),Page(s): 2352 – 2360
Yinghong Zhao; Xiao He; Donghua Zhou,"Optimal joint control and triggering strategies against denial of service attacks: a zero-sum game",IET Control Theory & Applications (Volume: 11, Issue: 14, 9 22 2017),Page(s): 2352 – 2360

[7] Kun Wang ; Miao Du ; Sabita Maharjan ; Yanfei Sun, "Strategic Honeypot Game Model for Distributed Denial of Service Attacks in the Smart Grid",IEEE Transactions on Smart Grid (Volume: 8, Issue: 5, Sept. 2017),Page(s):
2474 – 2482

[8] Raphael Durner ; Claas Lorenz ; Michael Wiedemann ; Wolfgang Kellerer,"Detecting and mitigating denial of service attacks against the data plane in software defined networks",Network Softwarization (NetSoft), 2017 IEEE Conference, 3-7 July 2017

[9] Massimo Ficco ; Francesco Palmieri,"Introducing Fraudulent Energy Consumption in Cloud Infrastructures: A New Generation of Denial-of-Service Attacks",IEEE Systems Journal (Volume: 11, Issue: 2, June 2017),Page(s): 460 - 470

[10] Munazza Shabbir ; Muazzam A. Khan ; Umair Shafiq Khan ; Nazar A. Saqib,"Detection and Prevention of Distributed Denial of Service Attacks in VANETs",Computational Science and Computational Intelligence (CSCI), 2016 International Conference,15-17 Dec. 2016

[11] Huabiao LuBaokang ZhaoXiaofeng WangJinshu Su,"DiffSig: Resource Differentiation Based Malware Behavioral Concise Signature Generation", nformation and Communication Technology - EurAsia Conference ICT-EurAsia 2013: Information and Communication Technology pp 271-284

[12] Somesh Jha ; Matthew Fredrikson ; Mihai Christodoresu ; Reiner Sailer ; Xifeng Yan, "Synthesizing near-optimal malware specifications from suspicious behaviors",Malicious and Unwanted Software: "The Americas" (MALWARE), 2013 8th International Conference,22-24
Oct. 2013

[13] Mihai Christodorescu,Somesh Jha,Christopher Kruegel,"Mining specifications of malicious behavior",ESEC- FSE '07 Proceedings of the the 6th joint meeting of the European software engineering conference and the ACM SIGSOFT symposium on The foundations of software engineering Pages 5-14

[14] Li, Z., Sanghi, M., Chen, Y., et al.: Hamsa: Fast Signature Generation for Zero-day Polymorphic Worms with Provable Attack Resilience. In: IEEE Symposium on Security and Privacy (2006)

[15] Jun Yang ; Jiangdong Deng ; Baojiang Cui ; Haifeng Jin,"Research on the Performance of Mining Packets of Educational Network for Malware Detection between PM and VM",Innovative Mobile and Internet Services in Ubiquitous Computing (IMIS), 2015 9th International Conference,8-10 July 2015

[16] Mohamed El Boujnouni ; Mohamed Jedra ; Noureddine Zahid, "New malware detection framework based on N-grams and Support Vector Domain Description",Information Assurance and Security (IAS), 2015 11th International Conference,14-16 Dec. 2015

[17] Mohamed Yassin ; Hakima Ould- Slimane ;Chamseddine Talhi ; Hanifa Boucheneb,"SQLIIDaaS: A SQL Injection Intrusion Detection Framework as a Service for SaaS Providers",Cyber Security and Cloud Computing (CSCloud), 2017 IEEE 4th International Conference,26-28 June 2017

[18] Pratik Satam ; Douglas Kelly ; Salim Hariri,"Anomaly behavior analysis of website vulnerability and security",Computer Systems and Applications (AICCSA), 2016 IEEE/ACS 13th International Conference,29 Nov.-2
Dec. 2016

[19] Byron Hawkins ; Brian Demsky,"ZenIDS: Introspective Intrusion Detection for PHP Applications",Software Engineering (ICSE), 2017 IEEE/ACM 39th International Conference, 20-28 May 2017

[20] Parisa Alaei ; Fakhroddin Noorbehbahani,"Incremental anomaly-based intrusion detection system using limited labeled data",Web Research (ICWR), 2017 3th International Conference,19-20 April 2017

[21] Paul Marinescu ; Chad Parry ; Marjor Pomarole ; Yuan Tian ; Patrick Tague ; Ioannis Papagiannis,"IVD: Automatic Learning and Enforcement of Authorization Rules in Online Social Networks", Security and Privacy (SP), 2017 IEEE Symposium,22-26 May 2017

[22] M. Ridwan Zalbina ; Tri Wanda Septian ; Deris Stiawan ; Moh. Yazid Idris ; Ahmad Heryanto ; Rahmat Budiarto,"Payload recognition and detection of Cross Site Scripting attack",Anti-Cyber Crimes (ICACC), 2017 2nd International Conference,26-27 March 2017

[23] Jing Yu ; Dan Tao ; Zhaowen Lin,"A hybrid web log based intrusion detection model",Cloud Computing and Intelligence Systems (CCIS), 2016 4th International Conference,17-19 Aug. 2016

[24] Ankit Shrivastava ; Santosh Choudhary ;Ashish Kumar ,"XSS vulnerability assessment and prevention in web application", Next Generation Computing Technologies (NGCT), 2016 2nd International Conference,14-16 Oct. 2016

[25] A.M. Resmi ; R. Manicka Chezian, "An extension of intrusion prevention, detection and response system for secure content delivery networks", Advances in Computer Applications (ICACA), IEEE International Conference,24 Oct. 2016

[26] Melody Moh ; Santhosh Pininti ; Sindhusha Doddapaneni ; Teng-Sheng Moh," Detecting Web Attacks Using Multi- stage Log Analysis ",Advanced Computing (IACC), 2016 IEEE 6th International Conference, 27-28 Feb. 2016

[27] Ashan Chulanga Perera ; Krishnadeva Kesavan ; Sripa Vimukthi Bannakkotuwa ; Chethana Liyanapathirana ; Lakmal Rupasinghe,"E-commerce (WEB) Application Security: Defense against Reconnaissance", 2016 IEEE International Conference,8-10 Dec 2016

[28] Piyush Nimbalkar ; Varish Mulwad ; Nikhil Puranik ; Anupam Joshi ; Tim Finin," Semantic Interpretation of Structured Log Files ",Information Reuse and Integration (IRI),2016 IEEE International Conference 28-30 July 2016

[29] D. Seethalakshmi ; G. M. Nasira," Detecting and preventing intrusion in multi- tier web applications using double guard", Computing for Sustainable Global Development (INDIACom), 2016 3rd International Conference,16-18 March 2016

[30] Zhou Li ; Alina Oprea,"Operational Security Log Analytics for Enterprise Breach Detection" ,Cybersecurity Development (SecDev), IEEE,3-4 Nov.2016

[31] Mohammad Ashiqur Rahaman ; Cédric Hebert ; Jürgen Frank,"An Attack Pattern Framework for Monitoring Enterprise Information Systems",Enabling Technologies: Infrastructure for Collaborative Enterprises (WETICE),2016 IEEE 25th International Conference ,13-15 June 2016

[32] Xinlong Zhao ; Weishi Zhang,"Hybrid Intrusion Detection Method Based on Improved Bisecting K-Means in Cloud Computing",Web Information Systems and Applications Conference, 2016 13th,23-25 Sept.2016