International Journal of Applied Engineering Research
ISSN 0973-4562 Volume 10, Number 4 (2015) pp. 10767-10782
© Research India Publications
http://www.ripublication.com

Intrusion Detection and Prevention System for Zero-day Attacks: A Two Dimensional Approach

Er. Srinivas Mishra

Dept. of Comp. Sc. & Engg.,
GITA, Biju Pattnaik University of Technology, Bhubaneswar, India
srinivas_mishra@yahoo.com

Dr. Manoranjan Pradhan

HOD, Comp. Sc. & Engg.,
GITA, Biju Pattnaik University of Technology, Bhubaneswar, India
manoranjanpradhan72@gmail.com

Dr. Sateesh Kumar Pradhan

HOD, P. G Dept. of Comp. Science,
Utkal University, Bhubaneswar, India
sateeshind@yahoo.com

ABSTRACT

A well talked about topic these days is the zero day attack. Authors have spent countless time to name this phenomenon in different ways such as “zero hour attack”, “novel attack”, “unknown attack” or attacks for which patch or signature is not available in the intrusion detection and prevention systems. The intention behind this research is to design a system which generates signatures at the point of unknown attack occurrence. The proposal is to have a solution which contains software utility along with both the blacklisting and whitelisting databases. It is better that a zero-day antivirus service utilizes both the whitelisting and some useful features of the blacklisting method too. The “Two Dimensional Intrusion Detection and Prevention System (2D-IDPS)” ensures that any novel attempts to exploit the network is scrutinized, approved and only then allowed into the system. This also provides superior protection against zero-day malware threats if compared with the conventional methods.

Key-Words: Zero-day Attack, Unknown Attack, Novel Attack, Blacklist, Whitelist, Intrusion Detection and Prevention system

I INTRODUCTION

Malware's threat has become increasingly contagious and abundant in the industries plus the individual usage. The infected applications mostly cause leakage of crucial data to the access of the evil mind. Protecting the networks from the malwares is a demanding task in the responsibility of the IT administrators these days. The widely accepted method of protecting the networks from the malwares is the anti malware solutions that has pre-defined signatures. These anti malware solutions runs on the technique of blacklisting. However this method is useless during the well planned malware attacks on the zero-day. This problem gave birth to a modern technique called the whitelisting, which provides a better way of protection from the malwares on the zero-day attacks by permitting the entry of the legitimate apps, codes, web pages and other processes and their activities on the network. This whitelisting method follows a list of genuine applications and permits their execution while prevents the entry of other applications [1]. Due to the upward trend of malware existence, the organizations have become vulnerable by getting themselves exposed from different stand point like: confidentiality of data, it's non-availability due to erosion and the lost value of its leaked information due to the emerging attacks from the malwares. The anti malware industry for almost two decades have been relying on the blacklisting technique to protect the network from the threats. These services mostly follow a treasure of the pre-identified threats. And these services get updated on regular or periodic to ensure the pre-identified list is up-to-date. But the modern day's malwares makes the signature dependent blacklisting method useless against the well structured zero-day malware attacks. This weakness of the blacklisting method has given birth to a more sophisticated approach of whitelisting which had been the bread and butter for the professionals in the anti-malware industry for the past few decades. Research proves that whitelisting method is much better in protecting networks from the zero-day attacks by the malwares [2]. The white listing method permits only the listed or verified apps, codes, web pages and other processes and their activities on the network. Thus this method by its characteristics eliminates the possibility of damage done by the foreign bodies with harmful projections. Though the whitelisting technique sounds very promising, its maintenance and execution becomes a tedious task. Simply put; it is almost impossible to accommodate the whitelisting technique in an environment where the users need to run magnitude of new applications or update the existing ones in the machine on a daily basis. There are systems which generate the warning once the attacks initiates to replicate, spread, and multiply on the network. Subsequently block the spread of the threats by assigning a unique signature becomes the identity of that virus and can be recognized in future by the network security devices such as IPS, IDS and Firewall [3]. Creating shields against recurring and new born attacks is a problem that has become the nightmare of many IT practitioners these days. Stating about the taxonomy of the typical network intrusion detection tactics, "zero-day" worm problem can well be a family member as an exaggerated extension of the anomaly detection policy. However, the constructive evolution of zero-day network attacks have brought in such distinguishing characteristics that, it unifies itself from the anomaly detection policy and researches. At the outmost the research of zero-day threats and its importance was initiated from the identification and signature assignment methods [4, 5]. But the hit ratio, accuracy and success of the detection technique is lower than that of the failure rates. In reality, detecting the victims and naming signatures to them alone is not enough, as the recent trends show that the reality is quite opposite [6]. Infected apps or software are commonly spread through electronic mails, file loaders, chatting apps, games and what not? [7]. As a counter to this either dynamic or static analysis patterns of tracking the infectious software attacks on the servers, clients, networks or any such malware prone systems have become prominently abundant these days. These patterns can detect the attack of the malware at the early stage of infection when the foreign body tries to spread its web around the network and thus can save the system from lethal alterations [8]. In the modern era of web based application the trend of lethal attacks are also on hype. Majority of these attacks are witnessed in the processing of the BFSI (Banking and Financial Services Institutions) sector especially [1]. Gates et al. [9] suggested the phenomenon of customized whitelisting method to shield the machines from the vulnerability of virus attacks. In a typical example the whitelist is designed, maintained and updated by the instructions from the users. Thus the new application adopted to protect the machines from a lethal attack seems covered and the networks secured comparatively better [10]. The attack where the malware tries to alter the machines is more lethal because they can cause direct losses of financial status in the BFSI domain. These are also called as the phishing attacks. The service to track phishing attacks is mostly used by the BFSI. Talking about the browser shielding extensions shared by the antivirus firms; they are not effective enough, because they rarely provide any protections from phishing attacks. Even this problem can be solved by a whitelisting solution which lists the anti-phishing applications [11].

The rest of the paper is organized as follows. In the Section II, we summarize the related work. In Section III, we are dealing with a Two-dimensional Intrusion detection and Prevention system for zero-day attacks, and agreed to introduce and describe the details of the process. The Section IV deals with the implementation of the model in the form of an algorithm and its results. In Section V we conclude and envision future works.

II RELATED WORK AND LITERATURE REVIEW

Recent studies suggest that, on an average the vulnerabilities in the networking and other computing devices count more or less thirty to forty each month [12]. A list of vulnerabilities in the systems are identified and listed every hour. This subtle vulnerability in today’s world has given birth to the inevitable field of intrusion detection and prevention systems. For instance the ZASMIN (Zero-day Attack Signature Management Infrastructure) system can act as the host for the cyber threats and its action of replication by subsequently assigning signature to the alien that could be utilized by the security systems like IDS and IPS. The ZASMIN system champions the use of a few modern techniques which includes cautious traffic scrutiny, threat authentication, and instant signature generation [8].The two best fields in the malware attack tracking category includes “static procedure of threat detection” and “the procedure of automatic signature detection” [13]. In static procedure of threat detection, features of the application under scrutiny are utilized to track infectious code. A key advantage of static procedure of threat detection is that it can perform the task of detecting the malware without letting the malware to run its codes and make degrading alterations in the network [8]. The methodology of categorizing the possible threats and the regular or threat-less traffic is vital in the static procedure of threat detection. During the filtration the codes with features that can induce ‘rapid circulation attack’ or ‘scan time attack’, must get filtered out by the predefined standards [8]. Validation in the after-attack method checks whether the session is leading to new patterns which has infected components. On the contrary the after signature validation method is to check whether the session initiated by the newly identified signature, has any infected feature or not. Thus it is clear that the previous is a concept of validating the earlier and current mass of threats, whereas the latter is about validating suspicious traffic that can lead to a virus in future, by taking help of the newly named signature. Considering this fact the new era of protection against zero-day malwares is deviating towards the whitelisting technique as this provides superior performance [2, 14]. Another crucial drawback of implementing the signature based method is dealing with the database of the genuine applications, creating patch files to integrate with the machine and validating the certificates which are stolen from some other system which already faced similar sort of problem.

Loopholes in blacklisting services:

First and foremost; when a user updates his or her anti-malware application they provide access of their machines to the anti-malware provider who can exploit the user information. Two, these applications download updates every day which leads to higher data consumption and extra load on the CPU, RAM and other such appliances [2]. Having said that, these anti-malware applications do not shield the host from zero-day attack because they lack a validation methodology for the detection of anything apart from the available signatures listed in the repository [15].

Whitelisting- Concept of Protecting against Zero-Day Malware Attacks:

The whitelisting technique on a grassroots works exactly opposite of how blacklisting technique operates. The whitelisting method follows a database of those applications, extensions, web sites, and other such traceable elements that are allowed to be accessed on the network. While this method allows the genuine applications listed in the white list database, the applications other than those are denied access. For instance in a typical corporate environment there exists an email whitelisting, which is defined by the administrator and it allows only a set of predefined email extensions or addresses.

Whitelisting Vs Blacklisting:
Whitelisting method doesn’t require signature or software updates. Unlike the blacklisting method they can facilitate protection from the zero-day signature-less virus attack. There is no need of any periodic scanning of the machines which in case of blacklisting method results in slow down of the user machine. While the listed applications are allowed to run and execute operations, the other applications need administrator right to run in the user device. This also helps in tracking all the applications running in the machines and thus minimizes the risk of freeware installations which can lead to the manufacturer claiming for license cost. Most of the Intrusion detection methods when it comes to research or surveys mostly depend on signature tracking, where the system is built to detect known lethal attacks listed in the repository. But the blacklisting method by its design can’t detect the first time attacks or Zero-day attacks.

III TWO DIMENSIONAL INTRUSION DETECTION AND PREVENTION SYSTEM (2D - IDPS)

Though the whitelisting technique looks by far the better technique, there exist a few positive features in the blacklisting technique as well. No doubt the blacklisting method does not provide protection against the zero-day virus threats and the whitelist technique can be crucial in such cases. It is better that a zero-day antivirus service utilizes both the whitelisting and some useful features of the blacklisting method too. The anti-malware solutions usually run on blacklisting technique by listing all the malicious applications, web addresses, extensions, email addresses and other such elements and blocking the entry of malwares, Trojan horses, infected applications and viruses to an extent by doing a tally with the signature database. At the same time these applications use the whitelisting technique to validate the smoother and risk free entry of listed emails and applications.

The proposal is to have a solution which contains software utility along with both the blacklisting and whitelisting databases. To successfully implement the “Two Dimensional Intrusion Detection and Prevention System”, the user needs to maintain both the blacklisting and whitelisting repository of the legitimate entries in the form of application installation, run level malwares, websites and other such executables. Tracking the executables by the signature tracking method is mutually exclusive in nature. Let us consider the diagram to get a better idea about how this two dimensional approach works.

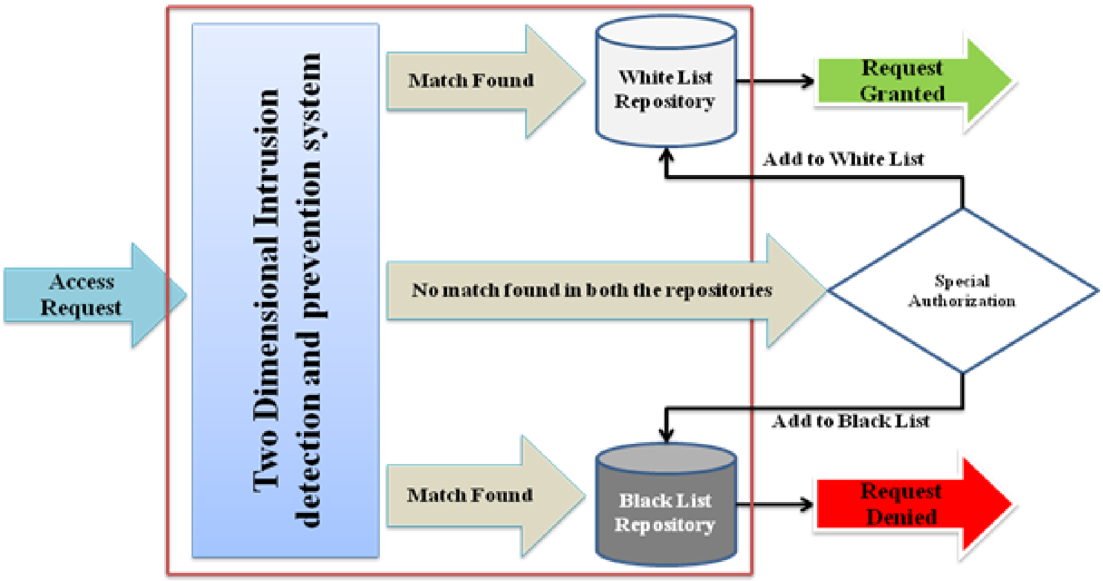


Figure 1: Two Dimensional Intrusion Detection and Prevention System for Zero-day Malwares.

Whenever there is incident where the user tries to access a website or application or code or any such executables, the access request runs through the “Two Dimensional Intrusion Detection and Prevention System”. The system initiates a process to check whether the same request already exists in either of the two repositories. In case a match is found in the whitelisting repository the access request is granted and the incident is closed. On the contrary if the match is not found in the whitelisting repository the system looks for its existence in the blacklisting repository. And if it is found in the blacklisting repository the request is denied and the incident is closed. That describes that the blacklisting repository and whitelisting repository are mutually exclusive in the two dimensional intrusion detection and prevention system. However if the access request doesn’t find a match in either blacklisting or whitelisting repository it needs to run through a special authorization. In case of user requires running an application or updating a service he or she has to take the admin rights in case the same was not listed in the whitelist repository. As shown in the diagram in our proposed model when no match is found in both the repositories the admin is requested for a special authorization. In this case if the admin approves the incident the access request is granted and the executable gets added to the whitelisting repository. Alternatively, if the admin disapproves the access request the access is denied and subsequently the executable gets added to the blacklisting repository. This helps in building the two dimensional database for future reference. As a result the “Two Dimensional Intrusion Detection and Prevention System” ensures that any novel attempts to exploit the network is scrutinized, approved and only then allowed into the system. Any suspicious executables can be well tracked and thus the network can be secured from sophisticated attempts to attack and exploit key information.

The tradeoff between whitelist method and blacklist method (Advantages of the proposed Solution):

The whitelisting section of the proposed application moderates the entry of any new malware attack in case the blacklisting repository lacks the information about it. The application to make its effect on the user machine needs administrator permissions as it is not listed in the whitelisting repository too. This system thus need not be updated using internet on both its whitelisting and blacklisting sections. The end users can be allowed for restricted usage of application and new application inclusions should be allowed only after passing admin rights. Due to the blacklisting and whitelisting combination there is no need for scanning the system periodically to track and wipe out malwares. This also provides superior protection against zero-day malware threats if compared with the conventional methods.

There can be an abnormality detection method where the system defines the normal or regular characteristics thus can detect the irregularity, which can potentially be the novel attacks. In this paper the two dimensional approach proposes a model which facilitates learning from past behaviors to strengthen the system in tracking both the blacklisted threats and at the same time can block suspicious entries. Firstly the system is able to learn algorithms which allow regular behavior in absence of the blacklisted attacks. Secondly it can also utilize a set of algorithms enabling it to look for the irregular entries which can possibly be a threat.

The experts from their experience have defined normalcy levels referring to earlier incidents and they design models that can track the deviation from the defined normalcy levels. The idea behind the “Two Dimensional Intrusion Detection and Prevention System” is to enable computers or the machine brains to detect abnormal behaviors like humans by utilizing a concept called “Data Mining” (through blacklisting and whitelisting repositories) from prior experience. It can be explained as a method, similar to how the acquired immune system works in the living beings. Forrest et al. [16] in their research referred that the immune system in living beings operates by detecting unusual foreign bodies and attacking them to protect the host. It is important to design the system in a way such that it not only detects the outside attacks, but the inside mutations also, because these can create potential alterations without triggering any alarm. Having said that; network based malware detectors can notify attempted attacks from outside at a very infant stage (even before it contacts the host) as compared to the host-based malware detectors [17]. Figure 2 is a workflow diagram that shows the working principle of the 2D-IDPS model.

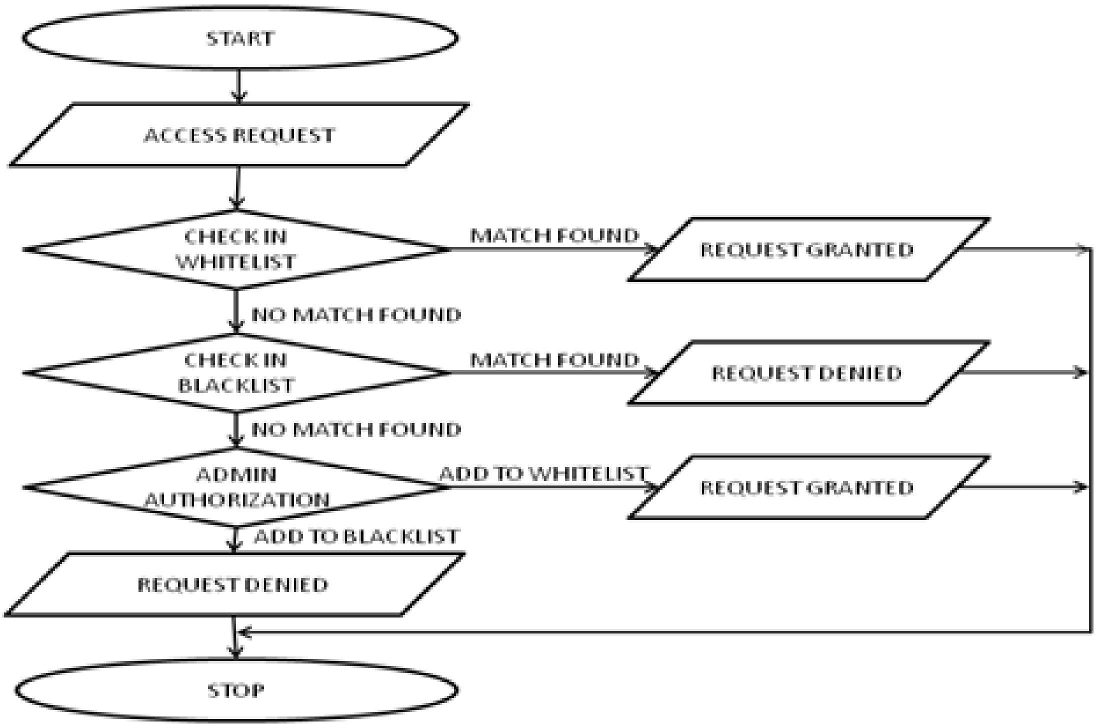


Figure 2: The Workflow Diagram for Two-Dimensional Intrusion Detection and Prevention System

Proposed Algorithm

Input: User Access Request
Output: Whether Request is to be Granted or Denied

Complexity:

$$\begin{cases} O(\text{logm}) & \text{If match found in Whitelist} \\ O(\text{logm+logn}) & \text{If match found in Blacklist} \\ O(\text{logm+logn}) + O(1) = O(\text{logm+logn}) & \text{If match not found in both the Lists} \end{cases}$$

2D- IDPS (R)

```
δ ← R
r ← Binary_Search(δ,WL)
if r = 1
allow δ and exit
else
r ← Binary_Search(δ,BL)
if r = 1
```

```
 deny δ and exit
else
a ← Admin_Authorization(δ)
if a = Y
Update(δ,WL)
else
Update(δ,BL)
end
```

Abbreviations

m ← Total number of entries in Whitelist repository
n ← Total number of entries in Blacklist repository
2D- IDPS ← Two Dimensional Intrusion Detection and Prevention System
R ← Resource
δ ← Holds the user resource access request
WL ← Whitelist
BL ← Blacklist

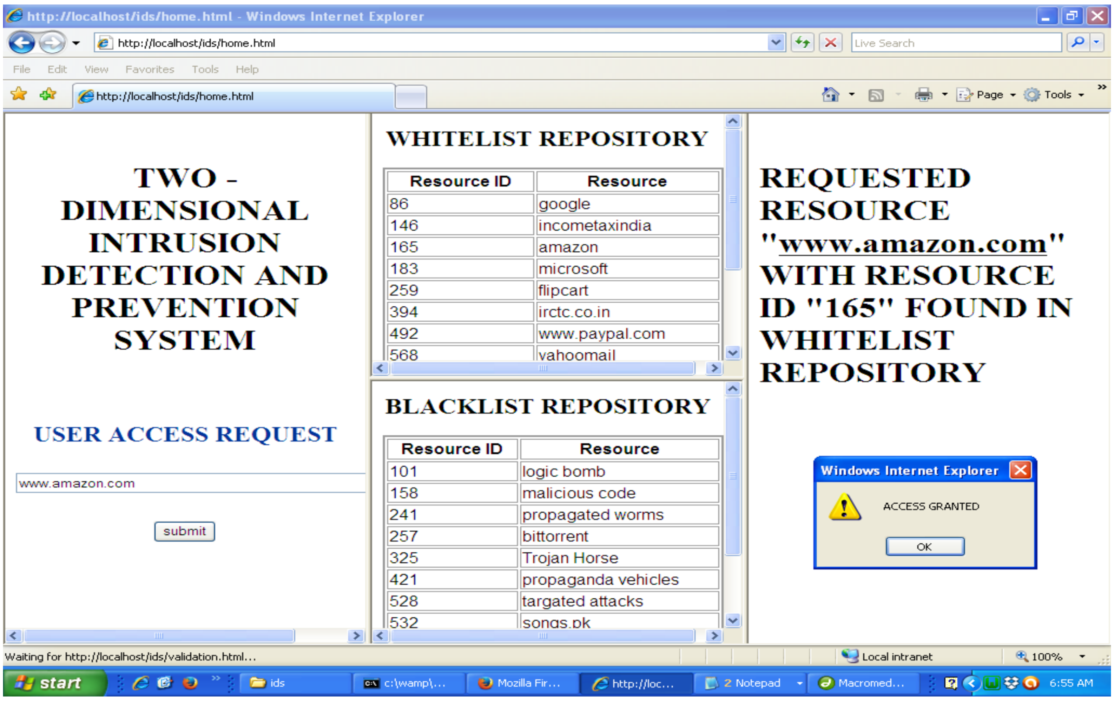
Binary_Search(Resource,Repository) ← This method search the resource(δ) in respective repository(WL, BL), if found it returns an integer 1 otherwise 0 and assigned to a variable r.

Admin_Authorization(Resource) ← This method ask to the admin for authorization if resource(δ) is not found in existing repositories(WL,BL). If allowed it returns a character Y otherwise N and assigned to a variable a.

Update(Resource,Repository) ← This method update the respective repository as per admin authorization.

IV IMPLEMENTATION

Proposed algorithm is implemented using web based PHP 5.4.16 and MySQL 5.6.12 database.


http://localhost/ids/home.html - Windows Internet Explorer
http://localhost/ids/home.html
Live Search
File Edit View Favorites Tools Help
Page Tools
Waiting for http://localhost/ids/validation.html...
Local intranet
100%
start
ids
c:\wamp\...
Mozilla Fir...
http://loc...
2 Notepad
Macromed...
6:55 AM

TWO - DIMENSIONAL INTRUSION DETECTION AND PREVENTION SYSTEM

USER ACCESS REQUEST

www.amazon.com

submit

WHITELIST REPOSITORY

Resource ID	Resource
86	google
146	incometaxindia
165	amazon
183	microsoft
259	flipcart
394	irctc.co.in
492	www.paypal.com
568	yahoomail

BLACKLIST REPOSITORY

Resource ID	Resource
101	logic bomb
158	malicious code
241	propagated worms
257	bittorrent
325	Trojan Horse
421	propaganda vehicles
528	targated attacks
532	songs.pk

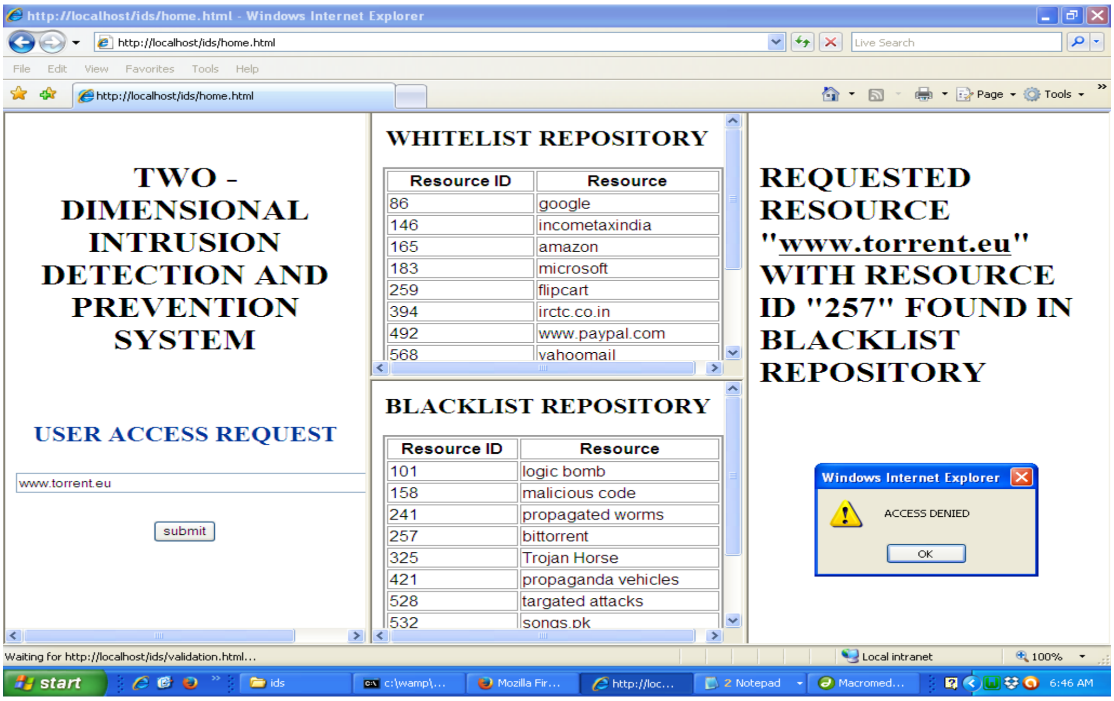
REQUESTED RESOURCE "www.amazon.com" WITH RESOURCE ID "165" FOUND IN WHITELIST REPOSITORY

Windows Internet Explorer

ACCESS GRANTED

OK

Figure 3: Screenshot showing access granted after match found in the whitelist repository


http://localhost/ids/home.html - Windows Internet Explorer
http://localhost/ids/home.html
Live Search
File Edit View Favorites Tools Help
Page Tools
Waiting for http://localhost/ids/validation.html...
Local intranet
100%
start
ids
c:\wamp\...
Mozilla Fir...
http://loc...
2 Notepad
Macromed...
6:46 AM

TWO - DIMENSIONAL INTRUSION DETECTION AND PREVENTION SYSTEM

USER ACCESS REQUEST

www.torrent.eu

submit

WHITELIST REPOSITORY

Resource ID	Resource
86	google
146	incometaxindia
165	amazon
183	microsoft
259	flipcart
394	irctc.co.in
492	www.paypal.com
568	yahoomail

BLACKLIST REPOSITORY

Resource ID	Resource
101	logic bomb
158	malicious code
241	propagated worms
257	bittorrent
325	Trojan Horse
421	propaganda vehicles
528	targated attacks
532	songs.pk

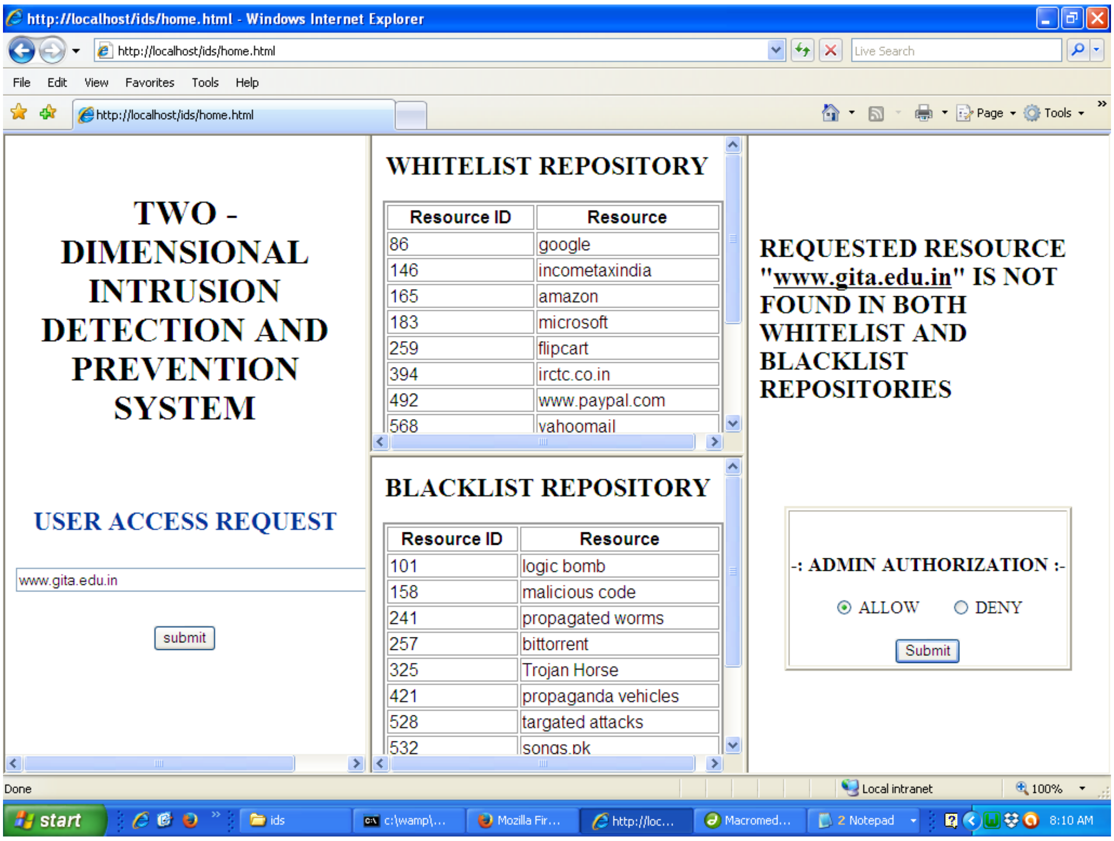
REQUESTED RESOURCE "www.torrent.eu" WITH RESOURCE ID "257" FOUND IN BLACKLIST REPOSITORY

Windows Internet Explorer

ACCESS DENIED

OK

Figure 4: Screenshot showing access denied after match found in the blacklist repository


http://localhost/ids/home.html - Windows Internet Explorer
File Edit View Favorites Tools Help
Page Tools
Done
Local intranet
100%
start
8:10 AM

TWO - DIMENSIONAL INTRUSION DETECTION AND PREVENTION SYSTEM

USER ACCESS REQUEST

www.gita.edu.in

submit

WHITELIST REPOSITORY

Resource ID	Resource
86	google
146	incometaxindia
165	amazon
183	microsoft
259	flipcart
394	irctc.co.in
492	www.paypal.com
568	yahoomail

BLACKLIST REPOSITORY

Resource ID	Resource
101	logic bomb
158	malicious code
241	propagated worms
257	bittorrent
325	Trojan Horse
421	propaganda vehicles
528	targated attacks
532	songs.pk

REQUESTED RESOURCE "www.gita.edu.in" IS NOT FOUND IN BOTH WHITELIST AND BLACKLIST REPOSITORIES

-: ADMIN AUTHORIZATION :-

● ALLOW ○ DENY

Submit

Figure 5: Screenshot showing admin authorization request after match not found in both whitelist and blacklist repositories

V RESULT ANALYSIS

The Whitelist (WL) and Blacklist (BL) repositories were constructed using the log file of Cyberoam firewall. Proposed algorithm is implemented using web based PHP with MySQL database in integration with Cyberoam web admin firewall with the following configuration:
Model No: - CR500iNG-XP
Firmware version: - 10.6.1 MR-2
IPS Signature version: - 3.12.3
Antivirus version: - 7.11.190.0
Web cat Signature version: - 0.0.0.187
Application Signature: - 4.12.3
Primary Memory: - 4 GB
Compact Flash: - 4 GB
HDD: - 250 GB

We observed the running of the algorithm individually without involving the Cyberoam firewall for a period of 3 days. The following graph (Figure 6) shows superior performance of the proposed algorithm compared to the Cyberoam firewall alone.

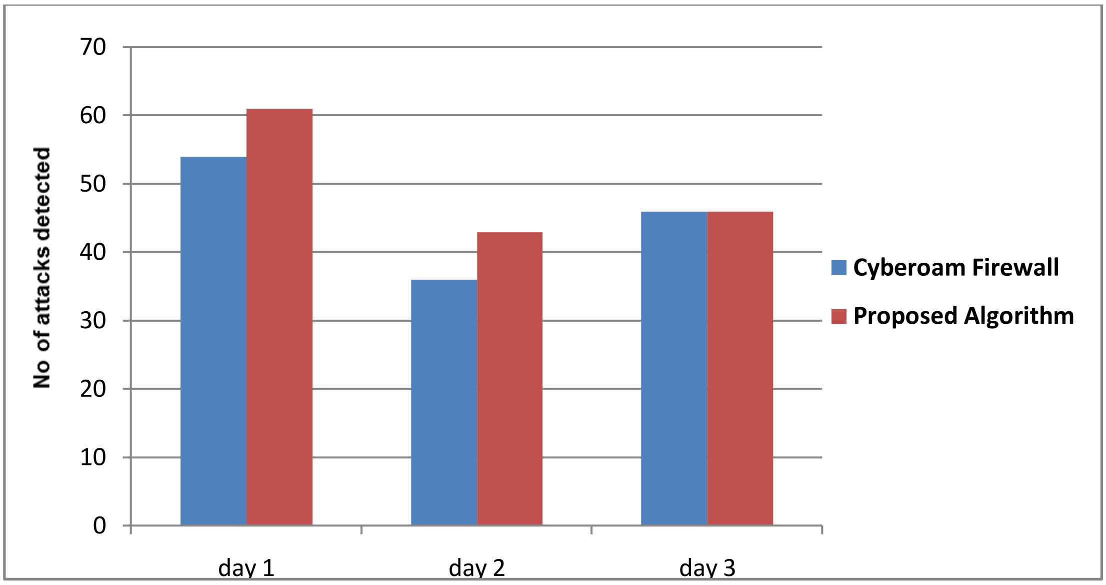


Figure 6: Proposed Algorithm against Traditional Cyberoam Firewall.

Again the firewall is observed with and without the proposed algorithm for 15 days. The firewall shows better results when combined with the proposed algorithm, as it is able to detect a wider range of unknown attacks including those which were not detected earlier by the firewall and were allowed into the network. These unknown attacks were allowed by the firewall as were not a part of the existing blacklist. However the 2D-IDPS adds another layer of security by requesting admin authorization and then lists it in either of the repositories depending on the response of the admin. The following graph (Figure 7) is a reflection of the results shown in the Cyberoam web admin console. The graph shows number of unknown attacks detected by the Cyberoam alone compared to the attacks detected by the Cyberoam in collaboration with the proposed algorithm.

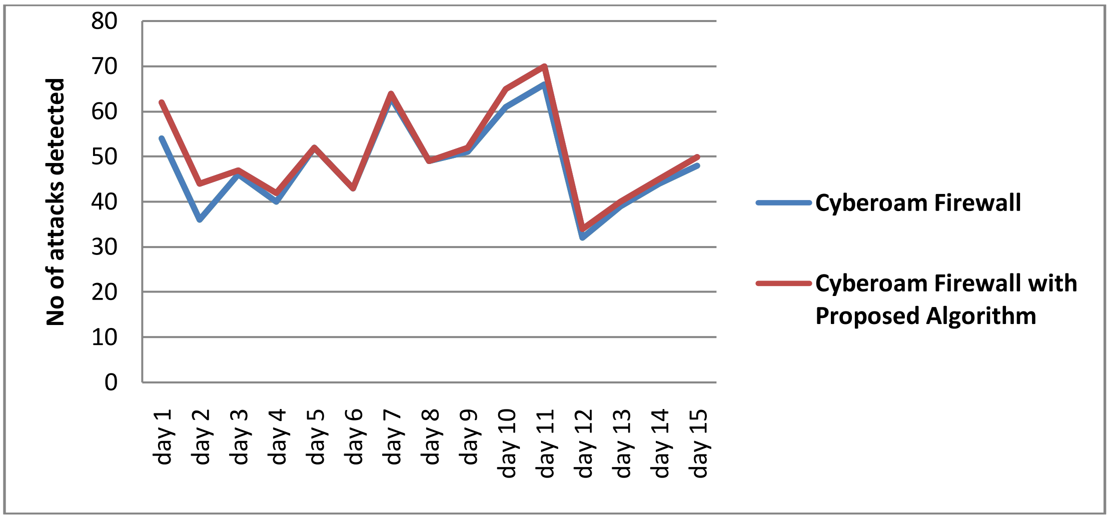


Figure 7: Proposed Algorithm along with Cyberoam Firewall against Cyberoam Firewall alone

VI CONCLUSIONS AND FUTURE WORK

In the initial part of this paper, we discussed about the destructive effects of the malware attack and its result in the form of massive data and information loss. Furthermore we discussed about the existing issues and limitations of both the signature dependent antivirus solution called blacklisting method and the credibility based whitelisting method. It's been years since whitelisting has been the only solution against the lethal zero-day attacks. Keeping this in mind, we have proposed the 2D-IDPS, an all in one solution that not only stands against the zero-day malware attacks but also takes care of recurring virus attacks like a traditional anti-malware solution. The intention behind this paper was to propose an all ends solution for zero-day attacks, shield against the malwares available in the blacklist repository and can be utilized for both home as well as large organizations. Referring to the implementation section and its results, we conclude that the 2D-IDPS solution provides superior shielding against both the signature based malwares as well as the zero-day attacks as compared to the conventional signature based blacklisting and whitelisting anti-malware solutions. Our future work is to train the system using soft computing techniques, so that at the point of zero-day malware occurrence the system automatically decides whether to allow or deny the traffic by matching the pre defined signatures and behaviors. Going forward, we envision enhancing our model to a level where it can be used in large organizations and enterprises to avoid intrusion into the system and add a new dimension to the security of networks.

Acknowledgments

This research is partially supported by Sangram Keshari Mishra, working at Technosoft Global Services (p) ltd, Bangalore and Prof. Sudhir Kumar Mohapatra, Gandhi Institute for Technological Advancement, Bhubaneswar.

REFERENCES

[1] A. Belabed, E. Aimeur, and A. Chikh, "A personalized whitelist approach for phishing webpage detection", 7 International Conference on Availability, Reliability and Security ARES, pages 249-254, 2012.

[2] Abid Shahzad, Mureed Hussain, and Muhammad Naeem Ahmed Khan, "Protecting from Zero-Day Malware Attacks", Middle-East Journal of Scientific Research 17 (4): pages 455-464, 2013.

[3] J. Bergeron, M. Debbabi, J. Desharnais, M. Erhioui, and N. Tawbi, "Static detection of malicious code in executable programs", Int. J of Req. Eng., 2001.

[4] J. Newsome, B. Karp, and D. X. Song, "Polygraph: Automatically generating signatures for polymorphic worms", In IEEE Symposium on Security and Privacy, pages 226–241. IEEE Computer Society, 2005.

[5] S. Singh, C. Estan, G. Varghese, and S. Savage, "The Early Bird system for real time detection of unknown worms", Technical Report CS2003-0761, UC San Diego, August 2003.

[6] C. Kreibich and J. Crowcroft, "Honeycomb – Creating Intrusion Detection Signatures Using Honeypots", In Proceedings of the Second Workshop on Hot Topics in Networks (Hotnets II), Boston, November 2003.

[7] C. Krugel, T. Toth, and E. Kirda, "Service specific anomaly detection for network intrusion detection", In SAC '02: Proceedings of the 2002 ACM symposium on Applied computing, pages 201–208, New York, NY, USA, 2002. ACM.

[8] Ikkyun Kim, Daewon Kim, Byoungkoo Kim, Yangseo Choi, Seongyong Yoon, Jintae Oh, and Jongsoo Jang, "An Architecture of Unknown Attack Detection System against Zero-day Worm", Proceedings of the 8th WSEAS International Conference on Applied Computer Science (ACS'08), pages 205-210, 2008.

[9] Gates, C., N. Li and J. Chen, 2012. "Codesheild towards personalized application whitelisting", 28th Annual Computer Security Applications, pp: 279-288.

[10] J.M. Kang and D.H. Lee, "Advanced whitelist approach for preventing access to phishing sites", International Conference on Convergence Information Technology, pages 491-496, 2007.

[11] Y. Wang, R. Agrawal, and B.Y. Choi, "Light weight anti-phishing with user whitelisting in a web browser", IEEE Region Five Conference, pages 1-4, 2008.

[12] I. Qualys, "The laws of vulnerabilities: Six axioms for understanding risk", In Qualys Whitepaper, 2006.

[13] W. Lee and D. Xiang, “Information-theoretic measures for anomaly detection”, In Proc. of the2001 IEEE Symposium on Security and Privacy, pages 130–143, May 2001.

[14] H. Pareek, S. Romana, and P.R.L. Eswari, “Application whitelisting approaches and challenges”, International Journal of Computer Science Engineering and Information Technology, IJCSEIT, pages 13-18, 2012.

[15] Faronics, “Blacklisting vs whitelisting software solutions”, Intelligent Solutions for Absolute Control Whitepaper, pages 1-6, 2011.

[16] S. Forrest, S. Hofmeyr, and A. Somayaji, “Computer immunology”, Comm. ACM, 4(10) pages 88-96, 1997.

[17] Philip K. Chan, Matthew V. Mahoney, and Muhammad H. Arshad, “A Machine Learning Approach to Anomaly Detection”, Technical Report CS-2003-06, Florida Inst. of Tech., Melbourne, FL, 2003.

Authors

Srinivas Mishra is a Ph. D. scholar in Computer Science & Engineering under Biju Pattnaik University of Technology, Odisha, India. He is presently working as an Asst. Prof. in the Department of Computer Science & Engineering, Gandhi Institute for Technological Advancement (GITA), Bhubaneswar, Odisha, India. His research interests include Computer Security, Intrusion Detection, Data Mining and Computer Architecture.

Manoranjan Pradhan holds a Ph.D. Degree in Computer Science. He is presently working as a Professor and Head of the Department of Computer Science & Engineering, Gandhi Institute for Technological Advancement (GITA), Bhubaneswar, Odisha, India. He has 16 years of teaching experience. He has published many papers in national and international journals. His research interests include Computer Security, Intrusion Detection, Soft Computing and Cloud Computing.

Sateesh Kumar Pradhan obtained his Ph.D. Degree in Computer Science from Berhampur University, India during the year 1999. He joined Berhampur University, as Lecturer in the year 1987 and promoted to Reader in 1999. He was Head, Post Graduate Department of Computer Science, Utkal University, India during 2001-2003. He was the Organizing Chair of the International Conference on Information Technology-2005. He served as a senior faculty in the Computer Engineering Department of King Khalid University, Ministry of Higher Education, Saudi Arab from September 2006 to July 2011. At present he is the Head, Post Graduate Department of Computer Science, Utkal University, Bhubaneswar, India. His research interest includes Neural Computing, Computer Architecture, Ad-hoc Networks and Computer Forensic.