INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY

ISSN: 2454-132X
Impact factor: 4.295
(Volume 5, Issue 3)
Available online at: www.ijariit.com

EVI-databse authentication using advanced security standards

Vaibhav Muthukumaran
vaibhavmuthukumaran@gmail.com
SRM Institute of Science and Technology, Chennai, Tamil Nadu

ABSTRACT

The concept of embedded virtual intelligence was to enable database authentication with advanced security standards. Data is the most resourceful asset of any information system the key idea of the paper was to secure data. Evi was designed with a centric algorithm that makes database authentication or access to any other system portal very secure. The functionality of this system is intelligently based on two major security modules are IP Retrieval Module and Automated Kernel Level Execution. IP Retrieval Module is a system package which runs on the background which has a steganographic implementation that retrieves the IP address of the host as soon as false login is attempted and logs I another independent server. Automated Kernel Level Execution Module overrides the system once the IP Retrieval Module is done this system force downloads executable files that run on startup now the executable files are implemented with kernel scripts that automatically retrieves all the network and system related information and packages it to a text file and mails back the details to the desired destination email address along the credentials. All these kernel scripts inside the exe files are encrypted by AES algorithm.

Keywords— *EVI-embedded virtual intelligence, Authentication, AKE-automated kernel-level execution*

1. INTRODUCTION

Database authentication is the process of finding that a user who is trying to log in to a database is authorized to do so, and is only accorded the rights to perform a task that user has been authorized. In EVI system where the user initiates secure start module he is directed to the login page, he/she is advised with the map showing the current location along with the detail assets like IP address, system name etc. This acts as a warning to the unauthorized users who may try to violate or void the security loop of the system.

When an authorized user tries to login he is redirected to IPRM and AKE, these are a system where a server responds with an awaiting page and then loads security breached image, this image has an algorithm running which retrieves his login credentials and other sensitive information and log them to another independent server. Meanwhile, this is a secondary security system that gets intercepted during invalid attempts and it forces downloads file and runs it these executable files retrieves user's details and mails back the details to the administrators'.

2. LITERATURE SURVEY

Database validation is an urgent part of any framework. Information being crude material, it's been between exchanged different hubs the framework present the present world give safety efforts that endeavour to avoid assaults over it yet at the same time we ran over many cases was security was undermined.

This is when we thought of a newer approach towards securing the system with not only advanced modules but also intelligently. This is when we introduced EVI that is Embedded Virtual Intelligence. EVI was a completely newer concept of safeguarding a system with a much higher chance of avoiding attacks over the system.

The most influencing reason for us to create EVI was the level of advancement that was provided by the innovation other systems were capable of retrieving and reviewing the system intruders after the acknowledgement of the primary attack which was different in our case EVI was capable to identify separate track and lock down the intruder.

In the further rolling out updates, we are trying to make EVI-self-aware where it would be independent of any backend codes and would be able to suspect and block access before even the intruder tries to attack the system.

2.1 System requirements

Hardware Requirements
Processor: Intel Pentium 4 and above
Hard Disk: 5GB
RAM: 256 MB
Monitor: 1366*768 (Recommended)
System Requirements
Operating System: Windows 7 and later
Front End: Adobe Dreamweaver, Chrome Browser
Back End: SQL Server (WAMP)
Language: PHP and Batch Scripting

3. EXISTING SYSTEM

Over the wide region organize like web there is a plausibility that a malevolent outsider can see the information that isn't proposed for them. The information can be gotten to by the outsider in the

event that they can break the security norms, essentially splitting the secret word. The current frameworks will just ensure that the unapproved client doesn't login into the framework, by asking clients certain security questions.

3.1 Disadvantages

There are a few weaknesses in utilizing the current system. They are:

- **Less secure:** The existing system provides only validation, neither does it track the location nor does it retrieve security and network information.
- **No counter security mechanisms:** The existing system provides only minimum security of two-way verification by sending security codes to the mobile number. This doesn't provide any advanced security.

4. PROPOSED SYSTEM

The concept of database authentication with security standards is that when there is an unauthorized usage from a third party system, it not only protects the unauthorized access but also locks down and blocks the unauthorized access with a special back end feature where a scripting code is embedded with an image which retrieves the network related information along with the login credentials. These logs are further encrypted by a host server system, for which the only accessing key is with the administrator. There is another standalone system which is backed up by another drive assisted download, all these systems are byte oriented and the kernel level module forward an automated download which also retrieves all the info with the enhancement of logging the system name and the logged on user.

4.1 Advantages

- A multilevel security system cannot be bricked at any time and so it is highly secure.
- Simultaneously it tracks the login credentials of the user and also blocks down the user so that he cannot proceed anymore.

5. MODULES IMPOSED

There are various modules induced to self-govern the system.These modules are classified accordingly as:

(a) Authorized Login Module: As soon as the user enters into the login page he is asked to give the desired username and password in order to login oneself. Meanwhile, the user can see MAP in the right side of the page denoting the current location access and all the details of his login credentials. In the event that the username and secret phrase are same, the client will be coordinated to the ideal administration page.

(b) Unauthorized Login Module: Suppose the username and password don't match then it will redirect to the login page for another attempt. In case the typed password entirely mismatches with the original password and a suspected attempt of the breach is found then the server will pretend to respond host, bit in the meantime the countermeasures will be activated by activating IPRM module and AKE system and sensitive credentials will be retrieved. The security credentials are retrieved by activation of two modules namely,

IP retrieval module: Using AREhost.server IP retrieval code is embedded on the back end of the image. In case of unauthorized usage, the user will be directed to a page containing this coded image. As soon as the user is being redirected to this page his entire security credentials are retrieved and the information can be viewed only by the administrator with a pre-shared security key. Hence the unauthorized user can be identified with his IP address and other credentials retrieved.

Login Failed: When the inappropriate user id and password are entered it gets redirected to a page with a security breached image. The page shows you are locked and the unauthorized user cannot proceed any more.

(c) ARE HOST.SERVER: ARE host. Server develops an image embedded scripting code page, where the user is redirected after unauthorized login. As soon as this image loads the user gets block down. The administrator gets all the information and has the right to access them only by entering the valid administrator password. Thus the login credentials of the hacker are retrieved.

(d) Steganography: This concept is used in EVISECSYS under IP retrieval module where the coded scripts are hidden under an image file.

(e) IP Retrieval and Storage: The IP address and the other system-related data are put away at the back-end.

5.1 Automated kernel level scripting module

The automated kernel level scripting module is triggered when the login fails due to the mismatch of user id and password. When the login fails, two clump records are consequently downloaded from EVISECSYS server. The batch files contain the kernel level scripting code, these codes with administrative privilege thus enabling easy access to the unauthorized user's system information. Since the batch files run with administrative privileges they start executing as soon as downloaded. The batch files contain codes to retrieve credentials from the system without the user's permission. The retrieved information is sent to the concerned administrator.

5.2 Login failed

When the user id and password don't match it gets redirected to a page with security breached image. The page says you are locked and the unauthorized user can proceed no more.

5.3 Forced download of the batch files

The Batch Files are auto downloaded as soon as login fails. This is accomplished by synching with EVISECSYS server which enables a forced download of batch files. The two batch files are:
A.exe: It retrieves the information from the unauthorized user's system.
Retrieve.exe: It sends the retrieved information to the Evisecsys server.

- **Execution of These Files:** These batch files execute with administrative permission so it doesn't require the user manual operation to run. It can start running as soon as it gets downloaded. All these batch file scripts are stored in the form of executable files.
- **Retrieval of Network Details:** With the execution of the code in the a.bat file the network credentials are retrieved. This retrieved information is sent to the Evisecsys server using retrieve.exe file codes. The retrieve.bat file contains the code for sending the retrieved code to the administrator.

6. IMPLEMENTATION

The development of EVI started off by creating an interactive and functional website. EVI security system has to be embedded before the login page of the website. If it is a dynamic webpage which keeps on refreshing every second making it difficult for hackers to hack.

The dynamic webpage was created by embedding two images. Each of these images rotates in the direction opposite to that each other's. Thus each time the image rotates the webpage gets refreshed. The start button on that web page will redirect to the login page.

In the login page if the email id and password matches then desired services are provided by the website. The website has been developed using HTML&CSS PHP adds functionality to the website.

If login failed then IP address and necessary credentials of the unauthorized user is retrieved. This is accomplished by two modules IP retrieval and automated kernel level scripting module.

6.1 IP Retrieval Module

The IP Retrieval module an ARE host server profile was created where an image was uploaded and embedded with IP address retrieval code. The image was linked to the loading HTML page.

6.2 Automated Kernel Level Scripting Module

The AKE two executable files were uploaded in the drives in case of a failed access of the system than these two files will be executed in the host system and the sensitive information will be retrieved.

6.3 Hosting of System

The complete system of EVI was managed to be wrapped within 10 MB of all space all the supporting files were uploaded to hostinger service in ftp and successfully hosted at evisecsys.eys.es

The linked database to the system was also uploaded in phpMyAdmin and the credentials were changed as accordingly.

7. CONCLUSION

In our opinion database authentication is a crucial transaction in the system wherein the most resourceful asset that is data is exchanged. Security is the major lead in the systems. The designed modules make sure that the system is completely secured neglecting all the possibility of security breaches.

7.1 Future Enhancement

Currently, EVI is in beta stage and capable of retrieving information and locating the host. We planned to extend our work and implement advanced features in the future stable releases of EVI. Features include:

(a) Instant lock down of the system
(b) Shutting down the system after retrieving the sensitive data.
(c) Making it cross-platform.

8. CODE

EVI working algorithm

```
Initiate securestartmode()
Validate the user{
  Give access to application protocol
Login(true)
{
Transcations()
}
Invalid login
{
Intercept user
{
Call IP retrieval module
{
Log user info to servers
}
Call Automated Kernel Execution
{
Force download .exe files
Autorun exe files
Mail back the sensitive details
}
}
}
```

9. RESULTS AND SCREENSHOTS

Following are the results.

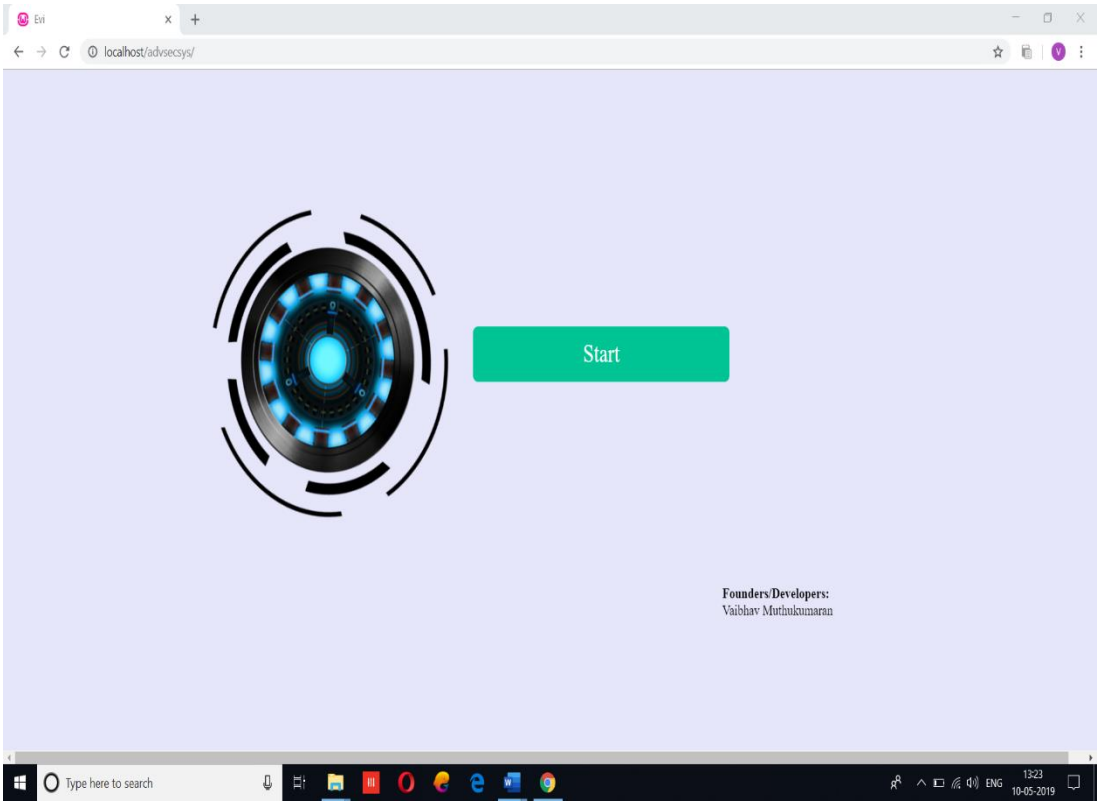

Fig. 1: Index Page

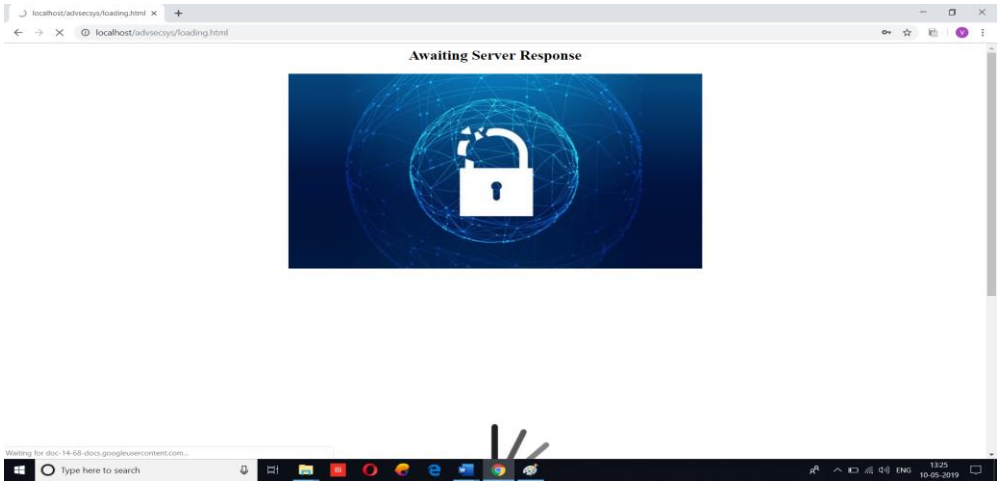

Fig. 2: Breached image [Steganography Implementation]

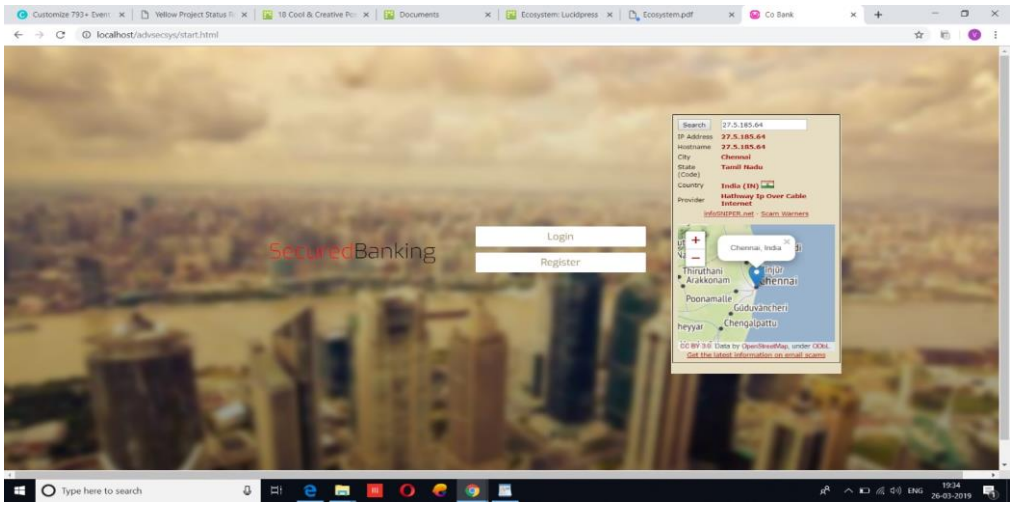

Fig. 3: Login Page

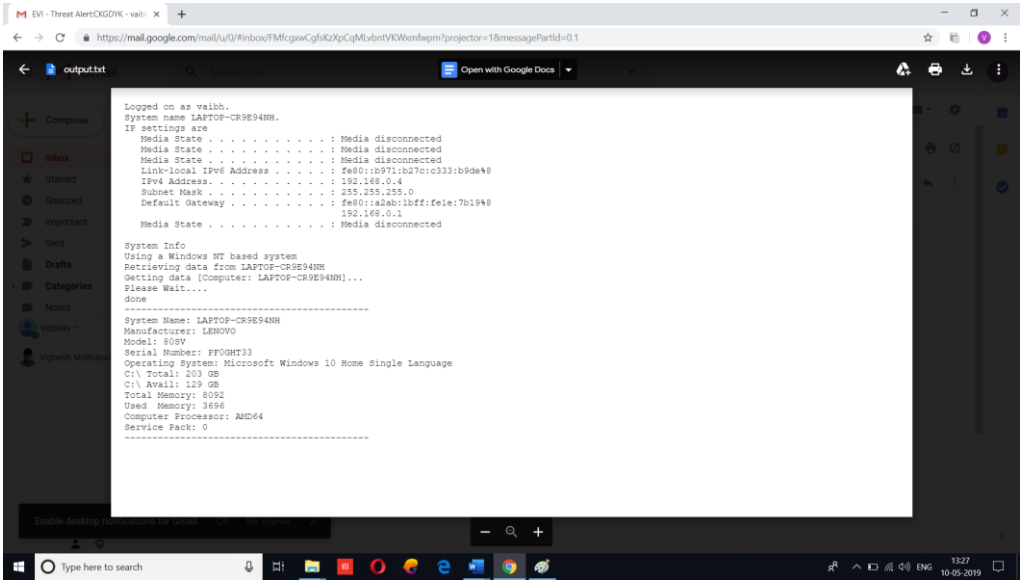

Fig. 4: Result sent to an administrator Email

10. REFERENCES

[1] S. K. Wajid{dot below}, M. Arfan Jaffar, Wajid Rasul, and Anwar M. Mirza, "Robust and imperceptible Image Watermarking using Full Counter Propagation Neural Networks" 2009 International Conference on Machine Learning and Computing, IPCSIT vol.3, 2011, IACSIT Press, Singapore, pp 385-391.

[2] Kumar et al Managing Cyberthreats: Issues, Approaches and Challenges Springer Publishers, 2005.

[3] Mr Saurabh Kulkarni, Dr Siddhaling Urolagin, Review of Attacks on Databases and Database Security Techniques, Facility International Journal of Engineering Technology and Database Security Techniques Research, Volume 2, Issue 11, November-2012.

[4] Shelly Rohilla, Pradeep Kumar Mittal, Database Security: Threats and Challenges, International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 5, May 2013.

