Software Architecture Tool to Detect and Prevent Intrusion Scripting in a Network

GRADUATE PROJECT REPORT

Submitted to the Faculty of
The School of Engineering & Computing Sciences
Texas A&M University-Corpus Christi
Corpus Christi, TX

in Partial Fulfillment of the Requirements for the Degree of
Master of Science in Computer Science

By

Ashwini Maligachari Achar
Summer 2012

Committee Members

Dr. Mario A. Garcia
Committee Chairperson

Dr. Dulal Kar
Committee Member

Dr. John Fernandez
Committee Member
ABSTRACT

The concept of using onion routing in wireless networks to hide IP address has triggered a lot of curiousness among the network users and also the administrators. Networks using onion routing fulfill the need of the users who demand the privacy of their IP address. These networks bounce data through a series of routers to hide the identity of the user and also their physical location. Some of the users really need this secrecy but some users are not worthy of it since their acts are abusive towards different websites. The administrators of these websites are unable to blacklist such users since their identity is not known. As a result they block the complete network using onion routing to ensure protection to their servers.

The proposed solution overcomes the latest enigma faced by the website administration due to the usage of onion routing networks. The System Administrators comprising of System Manager and Alias Manager, work in a synchronized manner to establish a secure connection between user, system software and server. The proposed software not only ensures the privacy of user’s IP address with respect to the server but also enables the system administrators to detect any malicious activity and further block the malicious user. The proposed system also includes a module to initiate Cross-Site Scripting Attack in the user module. The System Administrators are able to detect these attacks and block malicious users from accessing the system in future. Thus, the malicious users are not able to access any server data and also not able to violate any more rules and regulations.
TABLE OF CONTENTS

Abstract........................................................................................................................................... ii
Table of Contents............................................................................................................................... iii
List of Figures........................................................................................................................................ vi

1. Introduction...................................................................................................................................... 1

1.1 Onion Routing Networks........................................................................................................... 1

1.1.1 Phases of Data Movement.................................................................................................... 2
1.1.2 Routing with Proxy Aware and Non-Proxy Aware............................................................. 3
1.1.3 Security goals in Onion Routing Networks.......................................................................... 3
1.1.4 Advantages of Onion Routing Networks............................................................................. 4
1.1.5 Disadvantages of Onion Routing Networks.......................................................................... 4

1.2 Security Attacks on Web Applications...................................................................................... 5

1.2.1 SQL Injection Attacks......................................................................................................... 5
1.2.2 Cross-Site Scripting Attack................................................................................................ 5

2. Existing Systems........................................................................................................................... 8

2.1 Existing Secure Onion Routing Systems................................................................................ 8

2.1.1 Anonymous Credential System......................................................................................... 8
2.1.2 Pseudonym System ............................................................................................................... 10
2.1.3 Traceable Signature ............................................................................................................. 11
2.1.4 Blacklistable Anonymous Credential System................................................................. 12
2.1.5 Privacy-Enhanced Revocation with Efficient Authentication........................................... 13

2.2 Existing tools for detection of security attacks....................................................................... 15

2.1.1 Secure Web Application Proxy ........................................................................................ 15
6.1 Advantages ................................................................. 49
6.2 Disadvantages ............................................................. 49
7 Conclusion and future work .................................................. 50
8 Bibliography and References ............................................... 51
LIST OF FIGURES

Figure 1 Scheme of SWAP Setup .................................................................................................................. 15
Figure 2 The architecture of Ardilla .............................................................................................................. 16
Figure 3 Proposed mechanisms’ architecture ............................................................................................... 26
Figure 4 Successful access to System Administrator .................................................................................. 32
Figure 5 Unsuccessful access to System Administrator ............................................................................. 33
Figure 6 Successful User Login .................................................................................................................. 34
Figure 7 Unsuccessful User Login .............................................................................................................. 35
Figure 8 Activate System Manager ........................................................................................................... 37
Figure 9 Activate Alias Manager .............................................................................................................. 38
Figure 10 Successful Login .......................................................................................................................... 39
Figure 11 User accesses the list of files ....................................................................................................... 40
Figure 12 Initiate Cross-Site Scripting Attack ........................................................................................... 42
Figure 13 User accesses the list of files in Cross-Site Scripting Attack Mode .............................................. 43
Figure 14 User tries to access the files during cross-site scripting attack mode .................................. 44
Figure 15 Wireshark, the network protocol analyzer detects attack ............................................................ 45
Figure 16 Program extracts IP address of the user being attacked ............................................................ 46
Figure 17 The Malicious User’s IP address is extracted and added to the list ........................................... 47
Figure 18 Attacker through user tries to access the server files and blocked ........................................... 48
1. INTRODUCTION

1.1 Onion Routing Networks

Onion Routing is a terminology which is a new innovation and a complete new step towards wireless technology. It is the way for online private connections with enhanced security. The onion routing is the name of the software in which the data is encrypted into small packages and the message is sent. This message is completely protected from any other internet traffic along with all the hackers who are searching for any complex data and once they get their hands on it, they simply try to decipher it for fun and sometimes it can be because of some serious harmful business. This data is strongly protected as it reaches to the other side, which is further redirected to another recipient which deciphers; keeping the IP address of the sender completely concealed fulfilling the sender’s security demand. [Ryan 2011], [Xin 2009], [Paul 2001], [David 1999]

The name onion routing is given to the routing system because the design of the cryptographic message which is transformed in complex codes. The layers within layers theme is applied to the formula and each and every encrypted code is secured by another much stronger encryption so that if any outsider gets his hand on the message, the chances of which are really less, even then he is unable to take advantage of the message as he won’t be able to decipher it. [Ryan 2011], [Xin 2009], [Paul 2001], [David 1999]

The IP addresses are secured by using multi servers and with the combination of many routers which makes it very confusing for the tracker to know the original source. The recent improving techniques are making the security more complex to break in since it has become impossible to track an IP address because of the complicated encryption
and the coating of protection by the servers. [Ryan 2011], [Xin 2009], [Paul 2001],[David 1999]

1.1.1 Phases of Data Movement

The data movement through onion routing is based on three important stages or phases namely

- Connection set up
- Data movement
- Connection tear down

When the data is sent by the user, the message is layered into complex structure and the system is activated throughout all the routers. When the message is sent after the set up phase is completed, data movement begins and each layer is tore down as it passes from each router. The routers decipher the encryptions once the message keeps on passing through them securely and that is how the recipient receives the message in very simple text with its original form in which the message was sent. Thus these three steps are the confirmation of the security that the message will be transported in a completely secured way with no risks of getting intercepted between its way and will only be displayed when received by the recipient [Ryan 2011], [Xin 2009], [Paul 2001],[David 1999]
1.1.2 Routing with Proxy Aware and Non-Proxy Aware.

The onion routing is the software which can be used with a lot of options. There are a lot of protection tolls which encrypt the message sent by the system and there is no chance that the data can be located and then deciphered. To enhance the options, more data can be transacted in the onion routing by using both the proxy aware and proxy unaware applications like HTTP, SMTP, FTP etc plus it will also be applicable to those applications which are still being designed or are completely new launches likes DNS, NFS, IRC, HTTPS, SSH, NNTP etc. The vast applications of the onion routing are making it more and more successful day by day. That also includes the protection to those who might abuse the laws of the net and for that there are special tools and applications installed in the software which will easily back track the history of the user reporting the misuse by him accurately. [Ryan 2011],[Xin 2009], [Paul 2001],[David 1999]

1.1.3 Security goals in Onion Routing Networks

The protection word brings various structures of codes, but the main part of the protection is that it has to be simple and direct. The focus should not be diverted and the protection should be given to the most essential factors initially. The four simple points to keep in mind when a user is provided with privilege of concealing his IP address are:

- Sender activities
- Receiver activities
- Contents of sender
- Contents of receiver
Intruders who is trying to interfere must not be aware of these four details if the service provider desire the successful results of their services so that it is impossible to figure out that who is talking to whom and about what that person is talking to the other person who are both unidentified. That is why the basic protection method involves the distribution of the traffic nodes into multiple routers to confuse the intruder and misguide him from his path towards the original IP [Ryan 2011],[Xin 2009], [Paul 2001],[David 1999]

1.1.4 Advantages of Onion Routing Networks

1. The IP addresses are secured by using multi servers and with the combination of many routers which makes it very confusing for the tracker to know the original source
2. Even if a hacker or any other user tracks down the first server or router address even then it is impossible to proceed further
3. There is another complicated set of interlinked tracks in which only one of them leads to the next router hiding the identity of the user.
4. The user can access the system resource without any restriction with respect to his identity and physical location

1.1.5 Disadvantages of Onion Routing

1. The recent techniques are making the security more complex to break in since it has become impossible to track an IP address because of the complicated encryption and the coating of protection by the servers.
2. There are chances that onion routing could give protection to malicious user by hiding his IP address from the server administrator.

3. Server Administrator might block all the exit nodes of a particular onion routing network in the event of any malicious activity.

4. Legitimate and also illegitimate users are treated the same way and blocked from future access when the server administrator stops connection from a specific onion routing network.

1.2 Security Attacks on Web Applications

Web masters and application developers are experiencing an increase in security threats for web applications. The security attacks discussed are SQL Injection attacks and Cross-site scripting attacks. They help attackers to access the application without permission and steal sensitive data like banking information, credit card details, social security number etc. and use this information for illegal activities. The main reason for the web applications to be vulnerable to these attacks is that they trust the information provided by the user.

1.2.1 SQL Injection Attacks

This vulnerability is caused by non-validated user input provided to the database for execution purpose. The attacker embeds SQL commands in SQL queries and web application passes this query to the database. As a result, important data can be retrieved
and also un-authorized record can be viewed, updated and even deleted. By providing a suitably framed query, the intruder can increase the impact of this attack by damaging the information in the database and also execute some code on the server side. To protect web applications from this attack, the user input used in SQL query must be sanitized. If any potential threat causing commands are encountered, then such requests must be rejected [Kieyzun].

1.2.2 Cross site scripting attack (XSS)

The attacker takes advantage of insufficient validation of input/output provided to web application and inserts a JavaScript code on victim’s machine. The session data of victim is obtained and this information is further used on some e-commerce sites to steal crucial data. In this scenario the victim is impersonated by the attacker. In some scenarios, the victim is made to click on some URL which contains malicious HTML/javaScript embedded. This would result in retrieving the user cookies and other important information. To prevent this type of attack the user needs to cross-verify the link anchors of websites before accessing them. In addition to this, the application should not process any user input consisting of script code [Kieyzun].

1.3 Rationale

The proposed software helps the administrators to block certain misbehavior of users and retaining access to the users who use such networks in constructive purposes. This is achieved by recording the IP address and the alias name generated by the
software. In case of any malicious activity, the user is notified about its blacklisted status and blocks any further access to the server. This mechanism ensures that malicious users are not given any future access and the genuine users continue to use onion routing. [Eugene 2009], [Boukerche 2004], [MAN 2011], [Patrick 2007]

The security threat implemented in the proposed software is Cross-site scripting attack, using which attacker steals the session information of the user which could be later used to gain access to confidential information about the user and also threatens the server and the system software. This attack is detected using the network analysis tool. Based on the results from tool, system administrator blocks access to the user who has been affected to ensure the security of his confidential information and also to maintain integrity of the server.
2. EXISTING SYSTEMS

2.1 Existing Secure Onion Routing Systems

The concealed IP addresses of users makes most of the users a type of rule breaker as they get the feeling of being invisible and hidden behind a very strong mask which cannot be removed so they start breaking the rules of the websites and posting inappropriate comments, data and video clips as they know that the website’s administration will be unable to block them or take actions against them. The result is revealed as the website blocks all hidden IP address users or at least all the users from the same server. The authentication provider becomes blacklisted completely by the website instead of getting in the good books of advanced technology and getting appreciation. That is the reason behind the development of anti behavior software such that the websites can block the users without knowing their true identity. This is a step forward to maintain the technology in the good books of the cyber world and to keep the hidden mischief makers in control. [MAN 2011], [Patrick 2007]

The technologies which are currently employed to protect the integrity and the reputation of the servers are explained below.

2.1.1 Anonymous Credential System

The anonymous credential systems have presented the signature systems which are allotted by the group manager to the group members or the users. These signatures are traceable and whenever a user misuses his facilities the manager steps in and traces the
history of the user by the signatures as these signatures enables the manager to set a trap door through which the activities and the history of the user can be traced with keeping the anonymity of the user.

The signature system also holds lot of criticism that it might place the privacy of the concealed users at risk and that is why many different and efficient signature schemes are presented by different researchers, information technologists etc. The problem arises because the secret key which is kept by the signer is required to change between the invocations of the algorithms and the ideal random functions are the most remarkable signature schemes but these schemes are only applicable in the ideal structures, in the real system it is very difficult and requires many changes to make it successful. These schemes however can be used as the basic blocks or units for the cryptographic protocols and schemes. The latest scheme discussed has the basic solution of the secret key that it requires RSA assumption instead of the secret key but it is yet not reported as secure. [Jan 2004].

- **Drawbacks of Anonymous Credential System**

Anonymous Credential Systems uses the functionality of group signatures. The servers can complain about the misbehavior of a user to the group administration who would block the access to the user. The main disadvantage of the system is scalability, the server need to contact the group administrator for every authentication.

2.1.2 Pseudonym System
The private signatures, group signatures and private credentials are the three main methods of the pseudonymous credential system. The system was made to stop and to put control on the misbehaving actions of the hidden IP address users by providing a direct permanent system to the new or blacklisted users and providing them the services in form of pseudonyms. This way the users can get complete anonymity plus their actions are completely traceable by the service providers through pseudonyms. If the users start to misbehave then the service providers simply stop giving the pseudonyms to the users and blocking them from the services. There is no need to revoke them, thus reducing complicated methods to trace the history of the user. On joining the pseudonyms of the users and get the complete history of the user is obtained. This is a very successful formulization of anonymous blacklisting technique.

The status of the privacy can be selected by various privacy and security policies and the users are given credentials so that they can easily communicate with several other multiple organizations and communities without compromising their privacy however according to the level of security it is possible that some users have a low level of security and some of their information is under the risk of being revealed that is why it is necessary for the users to take all the precautions by enhancing the status of their security level by taking facilities from their service provider before communicating with other organizations or communities. The connection can be made form one credential to the other and the credential plays the act of resource of communicating but having the credential and communicating with the other organization through it makes the security of the users very low that is why the privacy policies can now be selected by the user to enhance the security. [Yuko 2006]
• **Drawbacks of Pseudonym Systems**

In Pseudonymous Credentials Systems, it assigns aliases to the users using which they login into servers. The servers can block the aliases of the users on the event of misconduct. Thus the purpose of anonymity is not achieved. Also it is very difficult to come up with a practical application scenario of using Pseudonym System by eliminating the constant communication between the entities. [Yuko 2006]

2.1.3 **Traceable Signatures**

In this mechanism, the data can now be signed like the documents of paper. The electronic signatures can be assigned to each user to put them on their messages instead of names and the encoded message will also contain their signature so the receiver will have the authentication about the sender without knowing the IP address of the user or any other identity related information about him. On the other hand there are group signatures too which a group or a network can use to identify itself and its users through the signature. The signature tactic also ensures the identity of the users who deal with the e-cash system and their identity secrecy can lure them away from their goals that is why the signature will keep them on the right track as their will be the risk of getting caught otherwise. [Stephen 2006]

• **Drawbacks of Traceable Signature**

These signatures are traceable and whenever a user misuses his facilities the manager steps in and traces the history of the user by the signatures. These signatures enable the manager to set a trap door through which the activities and the history of the
user can be traced with revealing the identity of the user after and also before malicious activity.

2.1.4 Blacklistable Anonymous Credential System (BLAC)

The top most priority of every anonymous service providers is to keep the anonymity of the users even if they are blacklisted or are going to be revoked. Most of the IP concealing services involve the trusted third party to reveal the identity of user so that the service remains unknown from the real identity of the user and the users IP is revealed along with his details but this is a very big drawback for the anonymous IP service providers because the main goal of these services is to keep the privacy and when the same privacy is not kept then there is no use of taking their services that is why the new technologies introduced enables the services to revoke the users without involving any trusted third party and revealing the identity of users is placed as the very last option when the person is involved in very serious criminal activities instead of misbehaving with various websites or double spending the e-cash. [Patrick 2007]

There are popular websites like YouTube and Wikipedia which provide specific tools to their users especially when it comes to Wikipedia which allows its users to make changes according to their preferences in the documents which allows the anonymous IP address users to violate the terms of these websites. The misbehaving user’s identity is revealed by the IP concealing services by involving the trusted third party however the punishment off revealing the identity just because of misusing the facility by violating the rules of the websites is too big although if the users start to go beyond their limits like double spending their e-cash then they can be punished by getting their IDs revealed that
is why the users don’t get the identity revealed just because of violating the terms of websites but are only revoked or blacklisted because the increased involvement of the Trusted Third Party decreases the standard and the security level of the IP concealing services. [Patrick 2007]

2.1.5 Privacy-Enhanced Revocation with Efficient Authentication (PEREA)

The IP concealing companies prefer to take actions against their users with keeping their identities in secret. They keep on trying not to involve any third party and without knowing the identity of a user they take actions against him. The PEREA is the completely new anonymous authentication scheme which is the modified and advanced form of the BLAC. It has a larger capability of revoking a list for a larger number of time unlike BLAC and its efficiency has been approved since it leaves no chance for the entrance of any third party because the third party’s participation means that the identity of the blacklisted user will be revealed which is against the rules and motives of the anonymous authentication software. The blacklisted members are however deprived from the membership with the company having the non membership proofs. The subjective blacklisting includes the privacy enhanced revocation and also the security of the users. [MAN 2011]

To enhance the performance and security of the anonymous service the service providers have launched the technology of tickets. These tickets allow the users the authentication to use the anonymous IP services securely and these tickets are approved and allotted to the users by the mangers of the service because these tickets provide the
history of the user and the ticket record is kept safe by the service providers as these tickets help to keep tabs on the users in case they try to misbehave by breaking the rules of the cyber world. With the help of these tickets the list of the users who are supposed to be blacklisted due to their behavior is made easily with fair tracing and is kept safe plus there is also a plus point that the service provider managers also have the proof of the misbehavior done by the users so that their actions cannot be claimed and even if claimed then the claims are proved baseless. [MAN 2011]

The security assurance of the users of the anonymous services is very necessary. The users which are revoked and blacklisted should not be able to get access with their anonymous IPs neither they should be able to use any kind of anonymous service provider’s services and facilities. There are also hackers and mischief makers who try to use these facilities without even becoming the member of the service so that they don’t even have to give any kind of information about them. These type of users are always having negative intentions and the security of the anonymous service providers should be very strong so that they can easily block such invaders. Another point which should be taken care of is that the involvement of the trusted third party should be avoided completely or should be decreased to a very low level so that there should be no threat against the security of the service so that the behaving users can feel completely secured in using the anonymous IP service. [MAN 2011]

2.2 Existing tools for detection of security attacks
The security attack detection tools namely Secure Web Application Proxy (SWAP) and Ardilla is widely used to detect SQL injection and cross-site scripting attacks.

### 2.2.1 Secure Web Application Proxy (SWAP)

SWAP is used to detect cross-site scripting attacks in web applications. SWAP works on reverse proxy mechanism, which controls the web information that should be protected from the attackers.

![Scheme of SWAP Setup](Wurzinger)

**Figure 1: Scheme of SWAP Setup [Wurzinger]**

As shown in Figure 1, the reverse proxy sends every response of the server to JavaScript detection component before sending it to client browser. This step is performed to detect the presence of embedded JavaScript content. All genuine script calls in the original web application are encoded into script IDs. If no scripts are detected by JavaScript detection component, then proxy decodes all scripts IDs and transmits the web response to the client. On the other hand, if scripts are found, then web response is not
sent to the client and instead a message indicating an attempt of XSS attack is sent [Wurzinger].

- **Disadvantages**

  The limitation of this tool is that it detects malicious content embedded only in Java based web applications [Wurzinger].

2.2.2 Ardilla

Ardilla is an automated tool to detect both SQL injection attacks and also cross-site scripting attacks in PHP/MySQL web applications to highest accuracy. It is used to detect vulnerabilities in PHP applications before the software is deployed to the users. The architecture of Ardilla as shown in Figure 2, consists of an input generator, executor/taint propagator, attack generator/checker and concrete and symbolic database [Kieyzun].

![Figure 2: The architecture of Ardilla [Kieyzun]](image-url)
- **Input Generator:** Generates a set of inputs with a goal to deal with various control flow path.

- **Executor/Taint Propagator:** Executes the application program on every input generated by input generator. The executor provides as output, a set of parameters (taint sets) whose values flow into each sensitive sink.

- **Attack Generator/Checker:** Uses the list of taint set to generate candidate attacks and to find out which among them co-relates to real attacks.

- **Concrete and Symbolic Database:** Can execute SQL statement both concretely and symbolically to detect XSS attacks [Kieyzun].

- **Disadvantages:**

  The limitation of Ardilla is that it detects security threats only in PHP based web applications.
3. NARRATIVE

3.1 Problem Statement

In general, when dealing with system incorporating onion routing, providing a secure communication is the most challenging task. The major concerns of users using the onion routing networks are:

- The user identity should not be disclosed in any circumstances.
- Irrespective of malicious activity, the genuine users should have access to the resources.
- In case of any malicious activity, the user identity should remain concealed for the transactions before any occurrence of misbehavior.

The major concerns of the servers using onion routing networks are as follows:

- To protect the integrity of the server system.
- To maintain the reputation of server system.
- Protect the server from any malicious activity by blocking access to abusive users.

Most of the existing system is not capable to meet all the users and also the server requirements. The systems which mainly focus on providing security to the server systems restrict the user from accessing all the resources and also monitors and tracks the user activities continuously. If any malicious activity is observed, then an entire set of exit nodes corresponding to a particular server are blocked, thus even the genuine users are deprived of using the resources from a server. The users hesitate to be a part of this system since there is no guarantee that their identity will be kept secret.
The systems which focus on providing the feature of concealing the identity of the user in most of the circumstances have comparatively weak security mechanism. This poses a very high security threat on servers since they are not able to identify the malicious users and also not able to take any action against the set of users accessing the server. Due to these reasons, sometimes the server needs to risk its reputation. The server administrators hesitate in participating in such networks which pose a threat on the integrity of server.

The concerns mentioned above is addressed to a major extent in the proposed system wherein the user is guaranteed that his identity would not be disclosed to the server or any third parties. The server administrators are also guaranteed there are minimal security concerns with respect to the server since the system handles the task of preventing the malicious users from accessing the system [Eugene 2009], [Boukerche 2004], [MAN 2011], [Patrick 2007]

### 3.2 Motivation

In today’s scenario, most of the user activity is done online. Each user is having confidential information or important data in the online accounts. Reports have been generated saying that many users’ data is leaked by the hackers and used for false purposes. This is causing a vital problem to the users of the system. Sometimes in the online accounts, there have been plenty of cases wherein the users’ security is compromised and the attacker got access to the resources. This would cause a drastic problem to the users because they might lose huge amounts of money or they might also lose confidential data which is very important.
Many reports say that intruders try to access personal or private information of the users using different types of attacks. Attackers try to gain the personal details of the user’s by using phishing activities and IP Spoofing. This has been causing many problems to the users personally as well as professionally. There are also hackers who would try to crack the users’ security mechanisms by applying probabilistic methods. Attackers find it extremely fun to work with or they find it something to boast about. The cheating practices implemented by the user also create many problems. There is no effective online monitoring scheme to record users’ activity.

All the above mentioned problems are occurring because of absence of an effective security and monitoring system. Even though certain software have been built to identify the IP address and block the users from future accessing the system, the situation discussed in the project deals with users using networks which hide the user’s identity. This has been the main motivation in implementing the proposed project. [Eugene 2009], [Boukerche 2004], [MAN 2011], [Patrick 2007]

3.3 Project Objective

The current project is developed to ensure secure communication in onion routing network between the server and user, when the identity of the user is not known to the server. The main focus of the proposed project is to achieve the following:
• **Protect server resources**

  The System Administrators ensure that any malicious activity in the system is detected and blocked such that it would not pose any threat to the security of the server.

• **Non-disclosure of user identity:**

  The system is designed such that even though a user is blocked, the identity of the user remains unknown to the server administrator or any third parties applications.

• **Un-interrupted access to genuine users:**

  The legitimate users of the system can always be sure that their identity will remain unknown and also that they would not be deprived of using any server resources due to some malicious activity in the network.

### 3.4 Functionality of the project

This proposed project can have various functionalities. The project can be used in various places. This project can be implemented in any location with an internet service provided the required software is installed. The misuse of the concealed IP address users have created a lot of problems for the anonymous software protection network that is why the blacklisting technique was improved and taken to a complete new level. The anti misbehavior system for the network is one of the most recent model in this criteria. The
specialty of this software is the successful grading of the blacklisted users. The local server keeps tabs on the users to catch their misbehavior and to launch its anti behavior system but it also blacklists these users on the local scale and stores this list while the directory server maintains all the lists from different servers and matches them to look for common blacklisted members and if he finds that the person has been messing around globally then that specific user is entered in the blacklist globally and this list is reported so that strict actions can be taken against them. [Ryan 2011],[Xin 2009]
4. PROPOSED SYSTEM DESIGN

4.1 Design and Implementation of a software tool to prevent access to malicious users

The current project is developed to ensure secure communication in onion routing network between the server and user when the identity of the user is not known to the server. The main focus of the proposed project is to achieve the following objectives:

- **Protect server resources:**
  The System Administrators comprising of System Manager and Alias Manager ensure that any malicious activity in the system is detected and blocked such that it would not pose any threat to the security of the server.

- **Non-disclosure of user identity:**
  The system is designed such that even though a user is blocked, the identity of the user remains unknown to the server administrator or any third parties applications. The user details are accessible only by the System Manager and Alias Manager.

- **Un-interrupted access to genuine users:**
  The legitimate users of the system can always be sure that their identity will remain unknown and also that they would not be deprived of using any server resources due to some malicious activity in the network.
4.2 Framework

The current project introduces a system which prevents future connections to user who accesses the server in a malicious way. There are various modules in the proposed system and maintaining the connection between the different modules is a challenging task. The proposed system does not include any front end software for the creation of Swing GUI. Instead it is implemented using Swing which is user friendly and also swing windows can be easily triggered by compiling and executing the corresponding java files in the command prompt. This makes the proposed system compatible with most of the server configurations since it does not have too many dependencies with respect to the environment settings.

4.2.1 Steps in the project development

The steps involved in building this project from the inception are given below in brief:

1. Building a graphical user interface
2. Server configuration
3. Creating modules
4. Linking the interdependent modules
5. Linking the applications with the database
6. User configurations
4.2.2 System requirements

Normally any computer installed with Java JDK 1.7, Tomcat 2005 server, Wireshark and Microsoft Access will be able to run this project. Sometimes the windows 7 64 bit version and also the 32 bit version are having some compatibility issues. This application runs best on windows XP operating system.

4.3 Proposed Mechanism

The proposed mechanism identifies and records the list of malicious users and also prevents them from accessing the resources in a server. The working of the system can be easily understood by having a look at the following Figure 3 which explains about the proposed architecture.
As shown in Figure 3, the major components of the system are System Manager, Alias Manager which can be together addressed as System Administrators. The user registration and server registration data are stored in the database. It can be observed that the user communicates with the Server and System Manager through a network which utilizes onion routing.

As it can be seen from Figure 3, the communication between the different components can be classified with respect to the user perspective and also the system perspective.
4.3.1 User Module

- **Registration phase**

  In the registration phase, the user provides all the information to Alias Manager. Alias Manager assigns an alias name to a particular user. Using this information, the user communicates with the System Manager and requests for a new user account creation. The System Manager, using his alias name gets all the details from the database which has been updated by Alias Manager and creates an account. User is notified with all the credentials including user id, password and user key which are required by him to access the server resources.

- **Login phase**

  At the time of login, the user is asked to enter the user id and password provided during the time of registration. In addition to user id and password, the user is made to enter a user key which acts as an additional level of authentication to access the resources in a server. It should be noted that, all users can login into the system to access the server contents. The only difference between the malicious users and genuine users is that malicious users will not be able to access the system resources but the genuine users can access all the resources assigned to the user. The user accesses the server resources through the System Manager and Onion Routing Network. This ensures that user’s identity is hidden from the server administrators who have only the information about the System Manager.
4.3.2 System Administrator Module

The system module basically comprises of System Manager and Alias manager, which have to collaboratively work towards preserving the identity of the user accessing the system and also providing security to the server from malicious users.

- System Manager

The System Manager is the major component of the proposed system which is also part of System Administrators of the whole system. The user registration and also the server registration are done by the System Manager. After communicating with the Alias Manager, the user contacts the System Manager for registration into the system. A new server, who wants to be a part of the proposed system, needs to communicate with the System Manager providing all the server details. The System Manager also has the authority to add the files into a particular server.

The System Manager has access to all the database tables and has all privileges to insert or update the database values. In case of any malicious activity, the System Manager gets the IP address from the database of the corresponding malicious user and adds it to the list of blocked IP addresses. Thus the server is not aware of the identity of the user and also the server is protected from any further misbehavior from the user. Thus, it also maintains a list of malicious users who are blocked from accessing the server. The System Manager contains all main control functionalities for the working of the system and every module need to work in collaboration with the System Manager.
• **Alias Manager**

The Alias Manager maintains the list of alias name of the users based on the IP address. The responsibility of the Alias Manager is to only to map the IP address to their corresponding alias names.

Alias Manager has the command over the user’s IP address, which ensures that a particular user can be prevented from accessing resource based on the behavior. The Alias Manager ensures that the same alias name is always assigned to the same IP address.

The Alias Manager also has access to the list of malicious IP addresses and whenever a user tries to login, it checks for the IP addresses in the malicious IP address list. If the user’s IP address exists in the list then it will not allow the user to access the server resources. If the user is a genuine user, then it provides access to the server resources.
5. IMPLEMENTATION AND RESULTS

The objective of the project is to provide users access to server resources, has been successfully achieved. The system always encourages legitimate users and provides all the required resources located in a particular server. Also, when it comes to the security of the system, system administrators do not always trust user. The system takes care of situations when attacks like cross-site scripting attacks are introduced and user becomes a potential malicious user.

In this scenario, the system software detects the malicious activity with the help of Alias Manager and System Manager. System Administrators detect the occurrence of the malicious activity and also the source of origination of such an attack at the user module. The System Administrators immediately block the malicious users and removes all access to servers. This ensures that the reputation and integrity of the server which is of high priority to the system is efficiently maintained. The results obtained are explained in detail in the following section with corresponding test cases.

5.1 Test cases and Results

The proposed project will now be tested for all the test cases sequentially. The following test cases will be tested.

- Verifying the System Manager access module
- Verifying the user login
- Verifying the user’s access to the documents in server
- Verifying the initiation of Cross-Site Scripting Attack
- Verifying the detection of Cross-Site Scripting Attack
- Verifying the user blocking functionality

5.1.1 Verifying the System Manager Access module

This is the most important aspect of the proposed project. In this section, the verification of the System Administrator Access module will be done. During the registration of the server, the server is assigned a unique server name and server key. Now two scenarios would be presented; one for a genuine System Administrator and the second one for a fraudulent System Manager.

The two scenarios for a successful and unsuccessful access will be shown with the help of the screenshots.

- **For a genuine System Manager**

  The login to the system is said to be successful, only if the server name and also the server key is correct.
Figure 4: Successful Access to System Manager

As shown in figure 4, the System Manager enters server name and server key to access the functionalities of a particular server’s System Manager. If the login details entered are valid, then the login is said to be successful. Upon, successful login, the user is redirected to the System Manager window of a particular server.

- **For a fraudulent System Manager**

  The login to the system is said to be unsuccessful, if either the server name or server key is incorrect.
As shown in figure 5, the System Manager enters server name and server key to access the functionalities of a particular server’s System Manager. If the login details entered are invalid, then the login is said to be unsuccessful. Upon, unsuccessful login, the user is redirected to the login page again.

**5.1.2 Verifying the user login phase**

This is the most important aspect of the proposed project. In this section, the verification of the user login credentials will be done. The registered user would be verified by presenting him with user id, password and also a server name in the
registration phase. Now two scenarios would be presented; one for a genuine user and the second one for a fraudulent user.

- **For a genuine user**

  The login to the system is said to be successful, only if the provided details are correct.

  ![Figure 6: Successful User Login](image)

  As shown in figure 6, the user enters user id and password to login into the system. If the login details entered are valid, then the login is said to be successful. Upon, successful login, the user is redirected to the list of files which the user has access to for a particular server. The Alias Manager takes care of the authentication of user credentials.
For a fraudulent user

The login by the user is said to be unsuccessful, if either the username, password or server name are not valid.

![Figure 7: Unsuccessful User Login](image)

As shown in figure 7, the user enters user id and password to login to the system. If the login details entered are invalid, then the login is said to be unsuccessful. Upon unsuccessful login, the user is redirected to the same login page.

5.1.3 Verifying the user’s access to the documents in server

After the authentication and verification of the user’s credentials, the user is able to access the files in a server when System Manager and Alias Manager are active. The steps to successfully access the file from the server is as follows:
- Activate System Manager
- Activate Alias Manager
- Enter user credentials in User Login Window
- Select “Access file” to view the files in a server

- **Activate System Manager**

  After the system administrator successfully logs into the system, the system administrator window is displayed as shown in Figure 8.
As shown in Figure 8, there exists a button named “Activate System Manager”, which is displayed above the list of malicious users. By selecting this option, the System Manager gets activated, this can also be checked on the command prompt which displays the message that “System Manager is running”. The System Manager is very essential component which maps the resources and the respective IP addresses of server and also the user.
• **Activate Alias Manager**

After the system administrator logs into the system, the option to activate the Alias Manager is displayed.

![Alias Manager Window](image)

**Figure 9: Activate Alias Manager**

The Swing window for the Alias Manager is as shown Figure 9. There are two buttons to start the alias manager and to stop the alias manager respectively. To ensure the mapping between the IP address and the alias names of the users, the Alias Manager has to be started before the user accesses the resources of the server. Alias Manager can be started by clicking the Start Alias Manager button as shown in Figure 9.
- **Enter user credentials at User Login Window**

  After the activation of Alias Manager and System Manager, the user can login into the system.

  ![User Login](image)

  **Figure 10: Successful login**

  As shown in figure 10, the user enters user id and password to login into the system. If the login details entered are valid, then the login is said to be successful. Upon, successful login, the user is redirected to the list of files which the user has access to.
• **User access files after successful user login**

The user login is done by entering the username, password and also server name of the server intended to access. The user needs to input his user id and password to successfully login. The user details entered should match the values in database corresponding to a particular user.

![Software Tool to Prevent Access to Malicious Users](image)

Figure 11: User accesses the list of files

After entering the user id and password, input dialogue box which asks the user to enter his server name is required for the user to access the files in a server. If the login is failed, the user needs to enter the login details again. After successful login, the list of files can be accessed by the user. As seen in figure 11, the user can select a file and click on the “Access File” button. Another swing window is displayed wherein the user can select the
“Click Here to Open Web Browser” and the webpage containing the files is displayed to the user.

5.1.4 Verifying the initiation of Cross-Site Scripting Attack

The steps involved in introducing a cross-site scripting attack towards the user module are as follows:

- Initiate Cross-Site Scripting Attack
- User tries to access server files
- User redirected to malicious page

- Initiate Cross-Site Scripting Attack

Execute the InitiateAttacker.java file to display a swing window which has option to enable and disable cross-site scripting attack.
Figure 12: Initiate Cross-Site Scripting Attack

As shown in figure 12, if the enable cross-site scripting attack is selected, a script is triggered which introduces cross-site scripting attack into the system. When the script is triggered and a malicious event has started, the user is unaware of this event and continues to access the server files as usual.

- **User tries to access server files**

  The user is ignorant of the existence of the cross-site scripting attack at his module and continues to access the server and the server files as in normal scenario.
Figure 13: User accesses the list of files in Cross-Site Scripting Attack Mode

As shown in Figure 13, the user tries to access the files and is also redirected to the server page. The cross-site scripting attack takes place when the user performs a logout and again login into the system. The attack is also action even though user is already in a login session. Thus, the attack has been implemented in such a way that irrespective of the login session, the user is impersonated into a malicious user.

- User is redirected to a malicious page

User, unaware of the existence of cross-site scripting tries to access files in the server.
Figure 14: User tries access the files during cross-site scripting attack mode.

The user logged in a particular session as shown in Figure 14, unaware of the attack, tries to access the files in server. The webpage opens as normal and the user tries to access the file by providing the user name and password. On clicking submit, the user is redirected to a malicious page which installs malicious software onto the system.

5.1.5 Verifying the detection of Cross-Site Scripting Attack

The steps involved in the detection of Cross-Site Scripting are as follows:

- System Administrators detect malicious activity through Wireshark
- System Administrator runs Check Attack script
- System Administrators detect malicious activity through Wireshark

The System Administrators continuously monitor the network protocol and traffic of the system using Wireshark, network protocol analyzer.
Figure 15: Wireshark, the network protocol analyzer detects attack

The System Administrators, who continuously monitors the incoming and outgoing data packets, detects an unusual activity that a non-registered user is trying to access the system resources as shown in figure 15.

- **System Administrator checks the “Check Attack” Status**

The System Administrator on detecting a request for transmission of data from malicious user, checks the attack status of the system.
Figure 16: Program extracts the IP address of the user being attacked

As show in figure 16, the System Administrator selects the option to “Check Attack” to generate a report of the user request connection status. This report is generated by a script which monitors the list of active connection, list of IP addresses and also list of connecting ports. Using this data, the System Administrator can confirm if there has been an attack or not.

5.1.6 Verifying the user blocking functionality

The steps involved in detecting the user who has been impersonated by Cross-Site scripting attack has been blocked are as follows:

- System Administrator extracts IP address and adds it to the list of malicious IP address.
- Malicious user is informed about the blocked status
• **System Administrator extracts IP address of the malicious user**

The system administrator checks Wireshark report and also the system generated report for the presence of any malicious activity.

![Image](image.png)

**Figure 17: The malicious user’s IP address is extracted and added to the list**

By parsing this report, the System Administrator extracts the IP address of the user though which the malicious activity is detected. As shown in Figure 17, the System Managers adds extracted user’s IP address to the list of IP addresses which have been blocked for further access to protect the system. This is achieved by selecting the option “Add Malicious IP”.

• **Malicious user is informed about the blocked status**

The user, who is unaware that he has been blocked, logs in successfully onto the server.
As shown in Figure 18, the user tries to access the file after successfully logging into the system. The user is prompted to enter the server name when he clicks on the “Access file” button. The user whose IP address has been blocked tries to access the file. Since the user has been attacked by an attacker and also already blocked, he is not given access to the file. The malicious user is informed with the pop-up window that he has been added to the list of malicious users. Thus in this system, the malicious user is also notified about the blocked status such that he would not access the server resources in future.
6. ADVANTAGES AND DISADVANTAGES

6.1 Advantages

There are many advantages in the proposed system. Some of them are as follows:

- The identity of the user is not revealed to the server administrator.
- Only the malicious user is detected and blocked from accessing the server resources.
- Legitimate users continue to access the server resources.
- The server is protected from threat posed by malicious users with unknown identity.
- Compatible with most of the server configurations.
- User friendly interface.
- Maintenance is easy.

6.2 Disadvantages

Besides all the above features, there are some disadvantages in the system.

- System Administrators has complete control over the application.
- Complicated database structure corresponding to each module.
7. CONCLUSION AND FUTURE WORK

The proposed system helps the server administrators to freeze the activities of users who perform certain malicious task and spoil the reputation of certain websites using onion routing networks. This is achieved with the implementation of System Manager and Alias Manager who work together to blacklist malicious users. In the event of cross-site scripting attack, the system administrators detect the attack and also successfully identify the user being attacked. The System Manager and Alias Manager block the user from accessing the server in future to ensure the security of user’s confidential information and also maintain the integrity of server. Thus, the proposed system meets user’s requirement by keeping the user identity hidden from the server and also fulfills the server requirement by blocking the malicious users.

The proposed system encourages users to utilize the benefits of using onion routing networks without the fear of getting their identity revealed due to the malicious activity of other users in a network. Also, it collaborates with the server administration to protect the servers against any threat posed to its reputation by malicious users, who employ onion routing technique in a network to hide their identity.

Apart from the work done towards the proposed design, my future work comprises of two main objectives.

1. First, is to develop an android application which will notify the System Manager when the blacklisted users try to access the server resources.

2. To generalize the system to detect various security attacks and block users who have been attacked to reduce the damage caused by attacker.
8. BIBLIOGRAPHY AND REFERENCES


