Proposing Operational Technology based Procedure (OTBP) using Round Robin Scheduling Algorithm (RRSA)

R.K. Seth
Department of Applied Sciences, Sri Sai University, Palampur, Himachal Pradesh (India)

Rimmy
Department of Computer Science and Engg, Sri Sai College of Engg.and Technology, Amritsar, Punjab (India)

Shubham Chuchra
Department of IT, DAV College, Abohar, Punjab (India)

ABSTRACT

This paper presents a review along with the analysis of different types of cyber hacking attacks and proposes a new methodology for reducing the attacks during client-server communication by providing a secure channel. The designed methodology is termed as an ***"OTBP-Using RRSA"*** ***(***Operational Technology Based Procedure-using Round Robin Scheduling Algorithm) and its working is based on the time of request entered on the search engine during client-server communication. It may help to provide security by automatic path encryption during request movement towards web server by following auto-generated unique hash address approach. The paper also discusses two different types of path hacking; viz. on-path hacking and off-path hacking by following different mechanisms such as path based authorization; path based traversing and path based access rules etc.

Keywords: Hash address, encryption, hacking techniques, round robin scheduling algorithm.

1. INTRODUCTION

As cybercrimes [8] and cyber-attacks [4] are increasing day by day, and securing personal information from the hackers is a great challenge for security professionals/ service providers. The security issue becomes more prominent especially during the development of any software. The hackers use several methods and strategies for stealing data and create varies of challenges for security providers. The strategies used by the security providers depend only upon the nature of attack. Generally, hackers utilize their knowledge and unethical skills for stealing any type of information. There are three different categories of hackers; viz. black hat hackers, white hat hacker and grey hat hackers with their own specific purpose for performing attack as discussed below:

- ***Black hat hackers:*** They are bad guys (Unethical hackers) with the purpose to bypass internet security. Such types of attackers also sometimes called "Crackers".
- ***White hat hackers:*** They are good guys and sometimes also called "ethical hackers" with the purpose to test the different networks and access their security. They are officially hired by multi-national companies.
- ***Grey hat hackers:*** They are skilled hackers and their activity lies between black hat hackers and white hat hackers and any activity depend on their specific purpose. Sometimes they use their strategies for improving the system and network security in real time. [9]

Security professionals are already divided hackers on the basis of their activity/ purpose that may either be ethical or unethical. For example; black hat hacker shows unethical behavior because they always target system for stealing information only and that stolen information will be further utilized for performing cybercrimes in future. Most commonly they perform penetration testing. The purpose of penetration testing is to target other systems that are connected with server machine and to steal available information from the target system that may be utilized anywhere or anytime in future [5]. They simply go through from initial 5- phases of hacking process where the function of each phase is distinct from the other phase as shown in fig.1:

Functions: Different phases of hacking:

Phase-1: ***Reconnaissance:*** Information gathering.

Phase-2: Scanning: Obtain target IP'S address and user accounts.

Phase-3: Gaining access: Enter into the network.

Phase-4: Maintaining Access: Owned system completely hijacked.

Phase-5: Covering Tracks: Evidences of attacks are destroyed. [6]

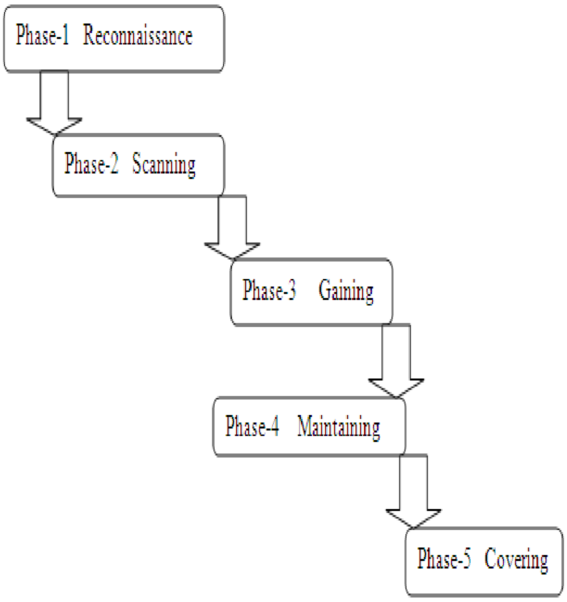


Fig 1: Phases of Hacking [1].

Utilizing above five phases of hacking, the hackers easily steal information and performs cyber-crime. The System administrators and security professionals need to focus on the methods and short-cuts used by the hackers for performing cyber-attacks. They may use separate levels where three most common levels; viz. system security level, data security level and network security level and are discussed below:

- ➢ ***System Security Level:*** It is mainly concerned with the boundaries between different computer networks.
- ➢ ***Data Security Level:*** This level deals with the data stored in the database. It is the duty of database administrator to provide safety to data from the destructive methodologies applied by the hackers.
- ➢ ***Network Security Level:*** It deals with the separate layers of different network models along with the most popular models such as OSI model and TCP/IP model. The function of both these models is network monitoring by using various security software's [2]

As professionals conducted a long survey on hacking and concluded that the actual structure and nature of hackers is not defined significantly. Structure can only be judged or *decided by the behavior and type of function performed. It may be legal or illegal. They may operate on loose social networks with limited number of users at two separate modes viz. online or offline [10]. According to their results, most of the attacks are to be performed on types of operations performed by using operational technology. By following different methods, mechanisms and techniques hackers easily copies the path; for example, by simply accessing registry files and also get the complete information of the types of operations applied that are related with specific path. So, to reduce the chances of attacks on path becomes mandatory challenge for security professionals and also an objective of this paper. For* performing path hacking, the hackers use two separate modes viz. ***"On-Path"*** and ***"Off-Path"*** that can be discussed below and is represented as shown in fig. 2 & 3:

- ○ ***On-Path hacking***: In case of on-path hacking, the hackers can easily intercept the traffic when data is being send during online mode e.g. phishing. It is a type of online fraud whose purpose is to steal money. Recently, phishing attack is performed on ICICI bank server in Oct, 2014 and is shown in fig.2 [16].

Fig.2: Phishing performed in ICICI Bank: Online Fraud. [16]

- ○ ***Off-Path hacking:*** Interruption is not allowed in case of off-path hacking that only supports non-preemptive environment. It actually makes an illusion for data transfer e.g. the use off-path hacking in TCP (Transmission Control Protocol) injection attacks and is shown in fig.3 [17].

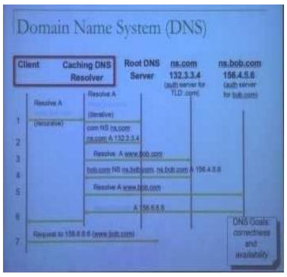

Domain Name System (DNS)
Client
Caching DNS Resolver
Root DNS Server
ns.com 132.3.3.4 (auth server for TLD .com)
ns.bob.com 156.4.5.6 (auth server for bob.com)
Resolve A
(iterative)
(recursive)
1
2
3
4
5
6
7
DNS Goals: correctness and availability

Fig 3: DNS Attack: Offline Fraud. [17]

Using these two separate modes, the path hacking will be easily performed by the hackers. The purpose of path hacking is to launch the path traversal attack. Due to the ease of implementation and consuming less time most of the time hackers prefer for launching path traversal attack using two steps that are discussed below:

Step-1)At first, Intruder manipulates the URL (Uniform Resource Locater) address in such a way that the web server executes or reveals the contents of a file anywhere or anytime on the server.

Step-2) After collecting the contents they follows the complete address of the outside document root.

For performing different path hacking attacks, attackers still may use number of ways. Some most common ways are listed below:

- Use of special character sequence in URL input parameters.
- Cookies.
- .../character sequence to alter the document or resource location etc.

To provide prevention from path traversal attacks, the concept of path traversal authorization is introduced. It gives the privileges to users to read or write on a certain directory or on repository. This paper considers files as path. So, the authors provide restriction on the access on files even where the hackers use number of hacking techniques for copying path and perform alterations. Four most common techniques are listed below:

- SQL Injection.
- Cross site scripting (XSS).
- File inclusion.
- Full path enclosure.

- ***SQL Injection***: It directly injects the databases for gaining an easy access of files. They may further apply several operations on databases e.g. modify, retrieve information and change privileges etc. Such types of operations are to be performed simply by executing SQL queries [11].

- ***Cross site scripting (XSS):***This technique uses a file of client side java script execution. Its main function is to steal cookies and some additional information which will be used in future for different purposes. Security professionals can easily identify such types of attacks with the help of “Alert Test” while running alert ( ) java script function.

- ***File inclusion:*** It helps to enable the attacker to get victim’s interpreter to load a given file that may either be loaded from the victim’s server or from another host.

- ***Full path enclosure***: This technique is used to supervise the complete path of any vulnerable script. It may include the unexpected/injected characters in the web page that helps to return an error message as well as operating path of the targeted script [13].

By applying above hacking techniques, hackers may easily perform hacking.

2. REVIEWING ANALYSIS OF CYBER HACKING ATTACKS

Most of the normal/end users are unaware from the different types of cyber hacking attacks. This review analysis that helps us for easy identification of attacks which are faced in our daily life and are listed below:

- ***By following the path of registry files*** that may perform attacks whose main function is to start a Trojan where Trojan is a type of malware that helps for launching attack.
- By ***analyzing the server file format***, hackers can easily copy the path by using path based access rules.
- ***Web browser*** can be easily utilized to copy sequential path for performing attack whenever any client send request to the server [3].
- By ***following digital forensic procedure***, the Security Professionals easily investigate the computer crimes that performed with the help of hacking [12].
- ***Normal file system*** can be used by the hackers for performing attacks.
- Path accessing can be easily determined by knowing all the possible communication paths into the network. Hackers mostly use ***off-the-shelf hacking tools for launching various attacks*** because of due to the ease of implementation.
- By usin***g various transport mechanisms,*** data packet monitoring can be easily applied on the network that in future leads to crime.
- ***With the help of network reconnaissance, hackers*** will easily determine the exact path of the network during accessing their path diagrams for port scanning and stack fingerprinting. These may help to determine the target host operating system.
- By following the ***path of DS*** (Domain server), hackers will easily copy path.
- By ***gaining access of DMZ*** (Demilitarized Zone), hackers easily perform attack. It is a kind of firewall configuration and utilized proxy servers that are use for securing local area networks.

After reviewed several cyber hacking attacks, security professionals have need to put their continue efforts to reduce these attacks by designing new methods and mechanisms [13].

3. REDUCING CYBER HACKING ATTACKS

The following strategies/mechanisms can be implemented to reduce several cyber hacking-attacks:

- ***Replacement of normal file system by the virtual file system*** that may create a difficulty *for the hacker to gain easy access of files.*

- **Use *global search and rather than normal search*** that helps to replace the actual code of all operations for accessing any file.

- By proposing a new algorithm that is termed as ***"Request handling Procedure".*** The function of this designed procedure is based on the selection of path or a channel. If any request is coming from any unexpected/ /unknown path, then it automatically discarded and break channel links. After that, the user will receive a warning message alert with specified details.

- **Apply *strong encryption algorithms* on registry files** so that the chances of copying path will reduce up to some extent.

- **Need to *design*** *personal/private firewalls* that may help to provide the facility of end-to-end encryption. It may also protect us either from a victim or attacker that use close proxy paths.

- ***By using the concept of directory server prevention,*** need to use operational environment in any co-operative network.

- It would be better to focus on operational technology rather than information technologies because of chances of attacks on operations are less.

- **By giving *local access of domains rather than global view of collaboration*** that actually provide us path authenticity. In addition, it also demands for the path discovery algorithm whose function is to discover a secure path in collaborative environment.

- Need to focus on the understanding of the concept of ***Access control lists (ACL'S)*** on firewall or router that helps to map all hosts on specific route to host Machine. The most common use of ACL'S is firewall testing or device testing.

- Prefer ***SAN (Storage area network)*** rather than any co-operative network due to tighten security because of it cannot be accessed directly as an example if any user wants to access specific route then he/she first connects with the external storage internet and take permission after that use it.

- Use ***concealed channels instead of normal channels*** to hide the path of sensitive areas that may provide a safeguard for escape routes.

By implementing the above discussed methods, cyber hacking attacks may be reduced.

The convergence between IT (Information Technology) and OT (Operational Technology) is always undertaken by IT professionals collectively. It may help to access path through various operational systems from the internet where the old OT systems were less secure.

*This paper overcomes the drawback of security over old OT systems and proposes a new designed methodology that is termed **as "OTBP-Using RRSA"** (Operational Technology Based Procedure using Round Robin Scheduling Algorithm) that helps to reduce the chances of attacks during client/server communication and provides a secure channel and is shown in fig.4.*

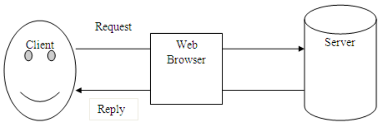


Fig.4: Two-Tier Architecture: Client/Server Communication.

This designed methodology uses the concept of hash Address for providing security during data transmission. The significance to use the concept of hash address is as under:

- It cannot be easily modified. If a message is to be modified then its hash should be changed and it no longer matches with the original hash value. The concept of hash address makes easy identification of attacker [15].

The basic structure of hash address includes the complete information of the key and value where key stores the actual hash address and value store the information that is to be transferred from the one place to another and is shown in fig.5:

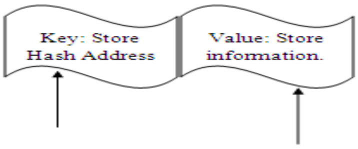


Fig 5: Hash Address Attributes (KEY, VALUE).

And two other major benefits of hash address are listed below:

- It is very easy to generate original hash address from the input data by using various algorithms and mechanisms that uses the principle behind PGP (Pretty Good Privacy) Algorithm for data validation [14].
- Very hard to generate fake hash address.

Fig.6 summarizes the steps to follow for enabling the proposed procedure for its implementation to reduce the chances of cyber hacking attacks in this cyber world.

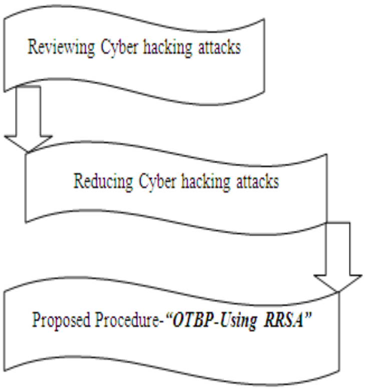
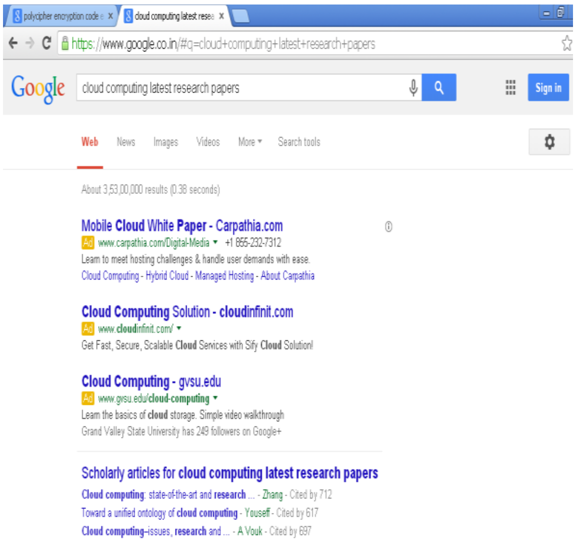

Reviewing Cyber hacking attacks
Reducing Cyber hacking attacks
Proposed Procedure-"OTBP-Using RRSA"

Fig 6: Steps for enabling proposed procedure.

Existing client/server communication methodology can be shown in fig.7:



https://www.google.co.in/#q=cloud+computing+latest+research+papers

cloud computing latest research papers

About 3,53,00,000 results (0.38 seconds)

Mobile Cloud White Paper - Carpathia.com
Ad www.carpathia.com/Digital-Media +1 855-232-7312
Learn to meet hosting challenges & handle user demands with ease.
Cloud Computing - Hybrid Cloud - Managed Hosting - About Carpathia

Cloud Computing Solution - cloudinfinit.com
Ad www.cloudinfinit.com/
Get Fast, Secure, Scalable Cloud Services with Sify Cloud Solution!

Cloud Computing - gvsu.edu
Ad www.gvsu.edu/cloud-computing
Learn the basics of cloud storage. Simple video walkthrough
Grand Valley State University has 249 followers on Google+

Scholarly articles for cloud computing latest research papers
Cloud computing: state-of-the-art and research ... - Zhang - Cited by 712
Toward a unified ontology of cloud computing - Youseff - Cited by 617
Cloud computing–issues, research and ... - A Vouk - Cited by 697

Fig 7: Existing Client/Server Communication: Path without using Hash Address.

Proposed client/server communication methodology is shown in fig.8:

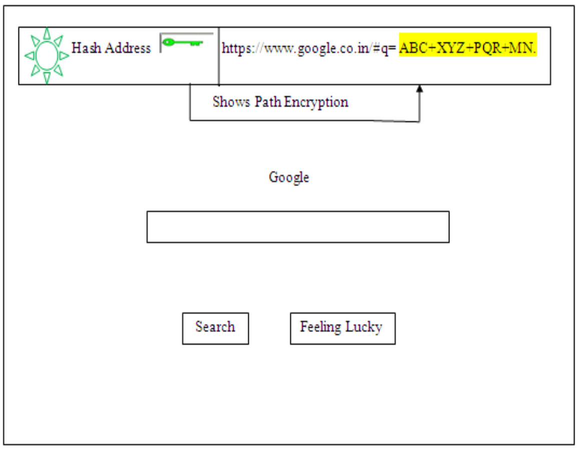


Fig 8: Proposed Client/Server Communication: Path using hash address provides automatic encryption.

4. DESIGNING METHDOLOGY

For providing prevention from hackers, this paper proposes a new procedure that is termed as ***"OTBP Using RRSA"*** ***(***Operational technology based procedure using round robin scheduling algorithm). Fig 9 shows the communication flow between client and server. As request proceeds from one location to another location then software automatically generate a unique hash address. The movement of hash address shows automatic path encryption by using strong encryption algorithms as an example SHA-256, 3DES, AES-256.

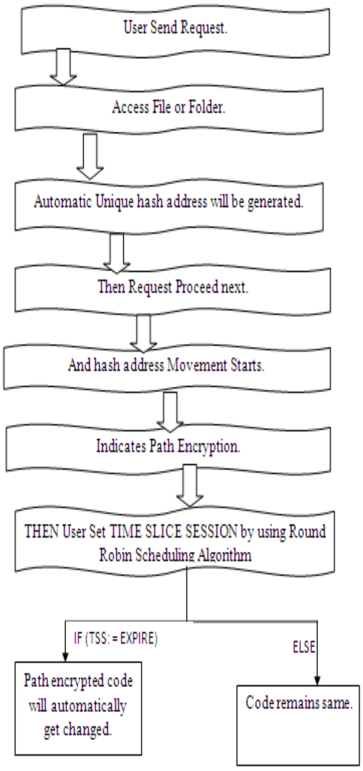

User Send Request.
Access File or Folder.
Automatic Unique hash address will be generated.
Then Request Proceed next.
And hash address Movement Starts.
Indicates Path Encryption.
THEN User Set TIME SLICE SESSION by using Round Robin Scheduling Algorithm
IF (TSS: = EXPIRE)
ELSE
Path encrypted code will automatically get changed.
Code remains same.

Fig 9: A Roadmap: OTBP-Using Round Robin Scheduling Algorithm.

5. PROPOSED PROCEDURE

Step 1) When USER SEND REQ: = ACCESS FILE THEN software automatically generate UNIQUE HASH_ADD.

Steps 2) AS REQ PROCEED: = HA_MOVE START.

Step 3) HENCE HA_MOVE shows PE by using strong encryption algorithm. [Triple DES-128 bit & AES-256]

Step 4) SET TSS: = O_HA! By using RRSA.

```
    IF (TSS: =EXPIRE)
        (
            Path encrypted code will automatically get changed.
        }
    Else
        {
            Path encrypted path code remains same.
        }
```

Step5) IF ATTACKER SEND: = REQ for CP! THEN ATTACKER FIRST apply algorithm to break the ENCRYPTED CODE after that hacker will copy the PATH and PERFORM HACKING ON OPERATIONS APPLIED.

Step6) END.

Table 1: Nomenclature in OTBP using RRSA.

PEC	Path Encryption Code
RRSA	Round Robin Scheduling Algorithm
OHA	On-Hash_Address
REQ	Request
3DES	Triple Data Encryption Standard
AES	Advanced Encryption Code
HA_MOVE	Hash Address Movement
PE	Path Encryption
CP	Copy Path
OA	Operations Applied
EA	Encryption Algorithm
TSS	Time Slice Session

6. WORKING

In the first step, when client sends request (as entered string on search box) for accessing any file through the internet, then software automatically generate a unique HASH ADDRESS. ***In the second step,*** as the request proceeds, hash address movement will start subsequently. In the ***third step***, the movement of hash address shows automatic path encryption by using any strong encryption algorithm. ***In the fourth step,*** set the time slice session on hash address by applying Round Robin Scheduling Algorithm. If time slice session got expires before request completion, then encrypted path code will be automatically changed, otherwise encrypted path code remains same. ***In the fifth step,*** if any attacker sends request for copying the path, then at first attacker must have to apply some strong encryption algorithms for breaking that specific encrypted code after applying several hacking techniques by following sequence of operations. It may either take long time to break the code or sometimes unable to break and depends on the types of mechanisms or techniques used by the hacker. Following the above procedure, the chances of attacks on path operations from hackers may be reduced.

7. CONCLUSION

A variety of cyber hacking attacks have been reviewed and analyzed. Cyber hacking attacks may considerably be reduced by developing the methodology ***“OTBP Using RRSA” a***nd follow the procedure as designed. The complete working of this proposed procedure is based on hash address where the movement of hash address provides automatic path encryption providing a secure channel during client-server communication. The proposed designed methodology in this paper provides efficient security mechanism rather than information based technology.

8. REFERENCES

[1] GurpreetK.Juneja, 2013. Ethical hacking: A Technique to enhance information security, International journal of innovative research in science engg and technology.

[2] Kumar utkarsh, Dec-2013.System security & ethical hacking, International journal of research in engg and advanced technology.

[3] White Papers: www.insecure.in/papers.asp.

[4] Moore, Robert, 2006. Cybercrime: Investigating high technology computer crime (is ted.).Cincinnati, Ohio: Anderson publishing.

[5] Wilhelm, Douglas, 2nd Professional Penetration testing syngress press.P.503.ISBN 978-1-59749-425-0.

[6] K.Balachoedappa, S.Subbalakshmi & P.N.V.S. Pavankumar, 2014. Ethical hacking techniques with penetration testing, International journal of computer science and information technologies.

[7] Mathieu Rehard, 2012.Practical IOS applications hacking, France.

[8] Ammar Yassur & Smitha Nayak, 2012.Cyber Crime: A thread to the network security, International journal of computer science and network security.

[9] Dr R.L Dave&sanjaymaheshwari, Challenges and prospects of ethical hacking, Indore, Madhya Pradesh.

[10] Thomas J.holt, Deborachstrumsky, June-2012.Examining the social networks of malware writers & hackers, International journal of cyber criminology.

[11] Mihir Gandhi &jwalantbaria, 2013. SQL injection attacks in web applications, International journal of soft computing and engg.

[12] Farhoodnorouzizadehdezfoli, Alidehghantanha&Ramlan Mahmoud, 2013.Digital forensic Trendz&future, International journal of cyber security and digital forensic: The society of digital information and wireless communication.[13]underurhat.Com/hacking/tutorials/introduction-to-hacking-techniques/.

[14] Hash-address: en.wikipedia.org/wiki/Hash-address.

[15] Identity Management and Access Governance Solutions - http://hitachi-id.com/.

[16] Phishing in banks, Images: https://www.google.co.in.

[17] Images for off path hacking: https://www.google.co.in.