International Journal of Security and Its Applications
Vol. 10, No. 8 (2016), pp.395-406
http://dx.doi.org/10.14257/ijsia.2016.10.8.35

DNS Prevention Using 64-Bit Time Synchronized Public Key Encryption to Isolate Phishing Attacks

Tanvi Gupta[1*], Sumit Kumar[2], Ankit Tomar[3] and KamalKant Verma[4]

[1]*M. Tech Scholar, Deptt. of Computer Science & Engg., Quantum School of Technology, Roorkee, India*
[2,3,4]*Asst. Prof., Deptt. of Computer Science & Engineering, Quantum School of Technology, Roorkee, India*
[1]*tanvi1011@gmail.com*

Abstract

In this work, a quick authentication scheme is implemented to prevent Phishing and DNS spoofing. In DNS spoofing, attackers inject the fake DNS server by duplicating the IP addresses and fake server redirect network traffic to wrong destinations. In phishing, phishers clone the legitimate website and user think that it is original website and users giving away their username and passwords to attacker's website and attackers hack their confidential information and they can misuse it for financial gain, identity theft, gaining fame, malware distribution and industrial espionage. We host the phishing website but we cannot pass the link through common hosting websites like Google and Facebook. So, phishers force the legitimate users to open a phished link with the DNS spoofing through fake DNS server then user directly redirect to a fake server. So our proposed work is to prevent DNS spoofing, to prevent the Phishing attacks by isolating it using 64-bit time synchronized public key encryption.

Keywords*: Domain name server(DNS), Internet Protocol(IP),Simple mail transfer protocol (SMTP), Transmission control protocol(TCP)*

1. Introduction

Every month the Phishing attacks are increasing in number and targeting the audience sizes that range from mass-emailing to lots of e-mail addresses around the world, to mainly targeted numbers of customers that have been enumerated through security flaw in small clicks-and-mortar retail websites. Phishers can easily dissipate customers into entering financial, personal and password information by using a key loggers, and number of attack vectors ranging from complete re-formation of a popular website to man-in-the-middle attacks. While spam is annoying, burden and distracting all its victims, phisher has shown the capacity to impose serious losses of information and direct losses due to malicious money transfers. With different cooperative improvement techniques to message delivery protocols such as experts extolling proprietary additions or SMTP, organizations may expect that the third-party fixes to be available before find out a solution to phishing.

While the security flaws within SMTP are really a popular exploit factor for phishers. For fraudulent message delivery, increasing array of communication channels is available. As with most illegal enterprises, if there is required money to be made through phishing, other message delivery avenues will be sought-after – even if the flaws in SMTP are eventually eliminates although this is probably to be happen within the next 3-5 years.

Internet fraud becomes a big threat as much as people depend on the Internet for personal finance, business and investment. Internet scams takes different forms, to

* Corresponding Author

ISSN: 1738-9976 IJSIA

opprobrious rumors that misrepresent stock prices, offered sale on online shopping websites from phony items, to frauds that promise high riches if the victim will help a foreign financial transaction by its own bank account. One of these Internet scam is phishing. In order to mislead victims into disclosing financial, personal and computer account data phishers use websites and email messages designed to seen as if they send by an original and authentic organization. Then phisher use this information for unauthorized purposes, such as larceny, fraud and identity theft. Users are misled into disclosing their information either by downloading and installing hostile software or by providing it through web.

The phishing attack includes three roles of phishers:

1. Attacker sends out a number of malicious emails that send victim to fraudulent websites.
2. Phishers collector configures a fraudulent websites, which forcedly bound victim to provide their confidential information.
3. Phishers Cashers use victim's confidential information to execute a pay-out. Usually pecuniary exchanges occur between those phishers. Figure 1 has shown the phishing information flow.

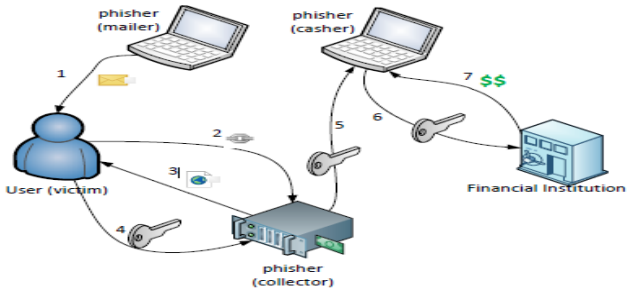

Figure 1. Phishing Information Flow

2. Phishing Techniques and Countermeasures

A. Email Spoofing

A spoofed email is the email that referred from one source when it was really sent from another. When a phisher transmits spoofed emails, including the sender address and other parts of the email header altered, in order to deceive victim this phishing technique is called 'Email Spoofing'. Spoofed emails mainly choose to be from a website in which recipient may have business with, so that a non-expecting recipient would chancily take actions as instructed by the email contents, such as:

- Enter your credit card number.
- Enter the password after prompted by the fake website including the link "view my statement".
- Enter confidential information into the form after open an attached PDF form.

B. Web Spoofing

A phisher actually use a website that seen resemble to an original website, so that victims may bound to think that this website is the genuine website and after this victim enter their personal information and passwords, which is hacked by the attacker . In the

today's web browsers there are an in-built security indicators are available that can secure users from phishing attacks, including https indicators and domain name highlighting.

However, they are usually ignored by careless users. Web Spoofing is done by making a fake website. By copying the front-end code it's trivial to clone of a website; it requires lesser amount of web programming to direct user's information into a file or database, and then pop up a notice of "website is under maintenance". To create a fully functional clone the software such as squid or Fiddler2 could be extended. Victim can properly sign in and use the services provided by the legalistic website, while all the information's are hacked by the fake server, and all the pages may be altered by the fake server.

The phisher must force potential victims to visit a fake website. There are a few ways to do this:

- Some spoofed emails are sent including a link to the fake website.
- By register a domain name that is a compositor of a common website. For example, register paypal.com and create a fake name paypel.com.
- By register a domain name exactly similar, but in a different TLD. Sometimes user will enter in their particular country-specific TLD and think to get a "localized" version of the website. For example, register yahoo.com.cn and create a simplified-Chinese forged version of yahoo.com.
- Use pharming
- By doing search engine optimization.

C. DNS spoofing

In DNS spoofing data is specified into a Domain name system name server's cache database, sourcing the name server to return a wrong IP address, redirecting traffic to attacker's system because of the open and distributed design of the DNS therefore it is vulnerable to various forms of attack. Attackers inject the fake DNS server by modifying the IP address. Now user send a website request to fake DNS server and fake DNS server open illegitimate website and users giving their personal information to fake website. The following diagram reflects this process.

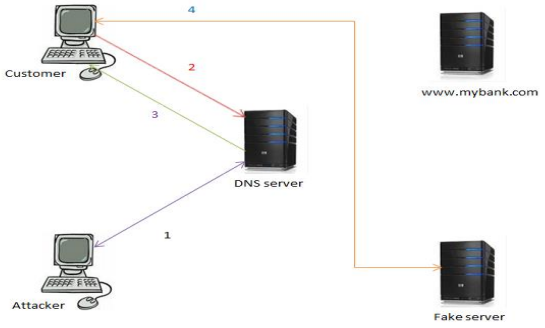

Figure 2. DNS Resolution Process Having Victim Fallen to a DNS Spoofing Attack

1. Attacker targets the DNS service used by the customer and change the entry for www.mybank.com — By changing the stored IP address from 160.10.1.21 to the attacker's fake site IP address (210.1.1.10).
2. After this customer asking the DNS server —"let me know the IP address of www.mybank.com?"
3. The DNS answers to the customer query with "The IP address of www.mybank.com is 210.1.1.10" — not the original IP address.
4. Then Customer is connects to the host at 210.1.1.10 —not known by the fact that customer is reaching the attackers fake site.

D. DNS Attacks with IP Spoofing

In these attacks the attacker send spoofed reply before the authorized reply of the query of the user and after this the original reply is discarded.

Sequential IDs

In DNS protocol TID is the main security process and have to be arranging randomly to intricate attacks. Because of this process, attack is become light, particularly on recursion enabled DNS servers. For determining the current TID an attacker only need to initiate a request to a name server, under his control. Attacker could send only few spoofed packets as per the following TID for a successful cache poisoning. The chances to send the right TID with a random TID are only 1/65535 (1/216) per packet as the TID has a range of 16bit. In the case of 50% successful attack, before the legitimate answer arrives the attacker requires to send more than 3MB of data with a packet size of 100 Bytes to the requester and it is even more lowered by 216-1024 chances If the server is using random source ports, so that's why the attacker has also to verify the right port in the range of 1025 to 65535. The whole possibility with random TID and port is 1/4.227.858.432 (< 1 / 0, 98*232). For that reason the quantity of data to be sent within time for a 50% chance is increased to nearly 200GB .It overworks a limitation in the reference to the fact that the most onymous DNS implementation (BIND) would send number of simultaneous recursive requests for the same IP address which was discovered in 2002 after all it is fixed in the recent versions of the software. It concludes "Birthday Paradox" could be mathematically increase the speed and probability of a successful attack by lessening the numbers of spoofed guesses of the DNS transaction ID from ten thousands reduce to a few hundred.

The Birthday Attack

It overworks a limitation in the reference to the fact that the most onymous DNS implementation (BIND) would send number of simultaneous recursive requests for the same IP address which was discovered in 2002 after all it is fixed in the recent versions of the software. It concludes "Birthday Paradox" could be mathematically increase the speed and probability of a successful attack by lessening the numbers of spoofed guesses of the DNS transaction ID from ten thousands reduce to a few hundred.

In the figure-3, the birthday attack is carried out as follows:

1. The iterative requests launched by the attacker to the DNS caching server for questioning "let me know the IP address of www.mybank.com" as frequently as possible.
2. At the same time, by using different DNS transaction ID's the attacker also sends repeated spoofed responses, statements "The IP address of www.mybank.com is 210.10.1.11.
3. The attacker in (1) for each request from the DNS server ,tries to resolve the IP address for www.mybank.com by asking the definitive mybank.com name server —commonly using a different DNS transaction ID. Because of the mathematical properties of Birthday Paradox, the attacker can "guess" a correct DNS transaction ID which is faster than the real name server can respond.

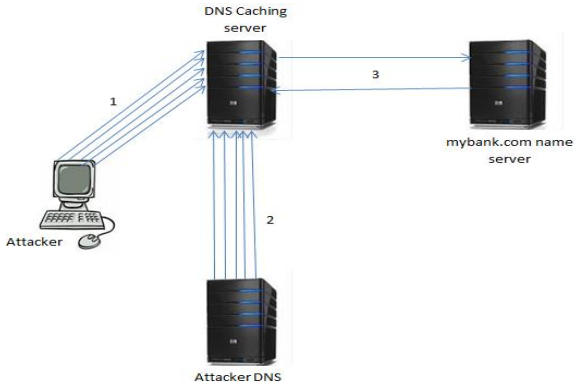

Figure 3. DNS Birthday Attack

3. Synchronized Encryption Technique and Result

A. Security Requirements

Our purpose is to develop an authentication scheme to prevent DNS server from DNS spoofing by isolate phishing attacks.

Our work has following properties:

- To prevent the user to phishers we used an encryption mechanism. In which encryption is done on the client side.
- To authenticate content from a server, we used decryption on sever side.
- This process will take very less amount of time because of using time synchronizing mechanics.
- It is hard for an attacker to hack the URL and unable to do further malicious activities.

We are using following security properties:

- In this interaction, the server provides security to the user, and the user provides security to the server.
- To provide authentication firstly we generate a public key in sever side then user enter an URL address and encrypt the URL with the help of key.
- Encrypted URL then transferred to server side and then decrypted by using private key. We enhance the security of infrastructure type of network.
- We are using 64-bit RSA Algorithm for public key encryption with the time synchronized mechanism because of that we can able to encrypt and as well as decrypt the URL that is requested by the user in less time period.
- Due to this time reduction in processing an attacker cannot be able to hack the information of the user by DNS spoofing.

B. Overview

We are using 64-bit RSA algorithm for public key encryption. First we need to know how it works.

RSA Algorithm

The most popular public key algorithm is RSA, invented by Rivest, Shamir, and Adleman and named as RSA. As the public and private keys RSA uses two numbers, e and d, as shown in Figure 4 [1].

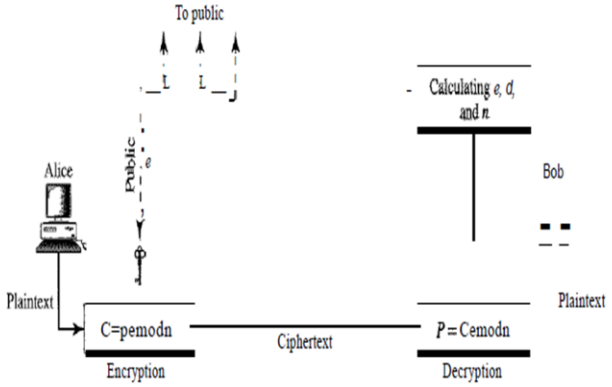

Figure 4. RSA

Working of RSA

Bob use the following steps to select the public and private keys:

- Bob selects two very large prime numbers p and q(a prime number is one that can be divided only by 1 and that number itself)
- Bob multiplies these two primes to find out the value of n.

$$n= p \times q$$

- Bob calculates another number.

$$\phi = (p -1) \times (q - 1).$$

- Bob selects a random integer e and then she calculates d so that

$$d \times e = 1 \bmod \phi.$$

- Bob declared e and n to the public and she keeps ϕ and d secret.
- In RSA, e and n are declared to the public and d and ϕ are kept secret.
- If a person needs to send a message to Bob can use NAND e. For example, if Alice needs to send a message to Bob, he can change the message, normally into a short form, to an integer. This is the plaintext. He then calculates the ciphertext, using e and n: C= P^e (mod n).
- Alice sends C, the ciphertext, to Bob.
- For Decryption Bob keeps ϕ and d private. When she receives the ciphertext, she uses his private key d to decrypt the message: P= Cd (mod n)

To implementing 64-bit RSA algorithm we have used VB dot net programming language. First step of our work is a key generation window. The second step is to enter an URL address and calculates an encrypted URL. After this in the third step DNS server decrypt the requested URL address and transferred the user to that particular address.

Key Generation

In Key generation DNS server generating a pair of public/private key before each time user will enter any URL address.

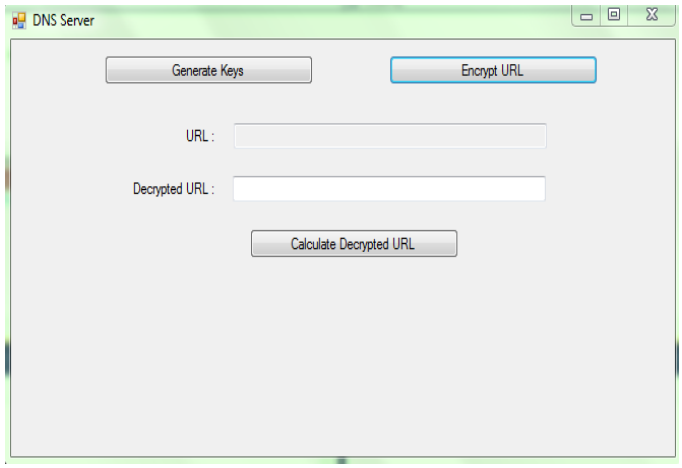

Figure 5. Key Generation

Calculation encrypted URL

After generating keys user enter an URL address and request the DNS server for the particular website.

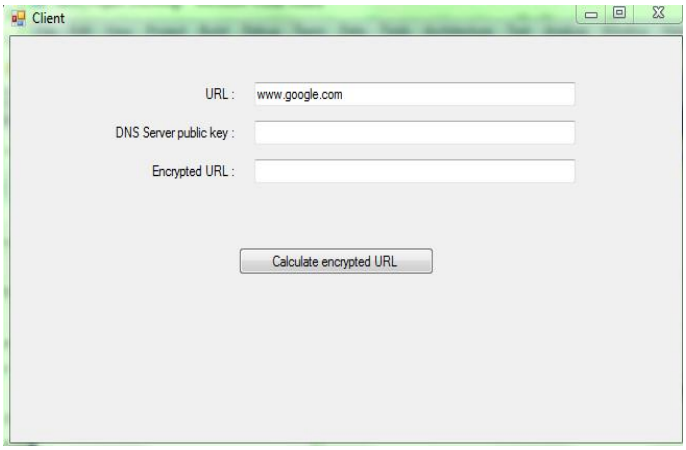

Figure 6. Encrypted URL Calculation

The requested URL is transferred to DNS server in encrypted form.

For example if we enter an URL address *www.google.com* then the *address* firstly encrypt and after this transferred to DNS server.

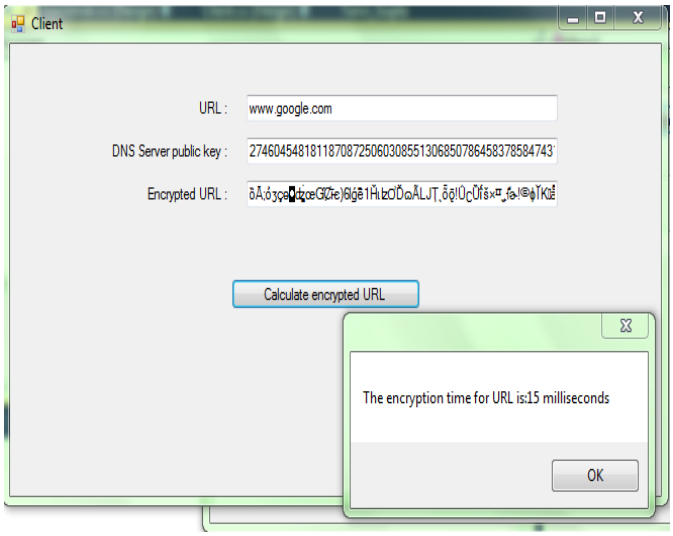

Figure 7. Encryption of *www.google.com*

Encryption process will takes very less amount of time because of our time synchronizing mechanism.

Now this encrypted URL address is transferred to DNS server.

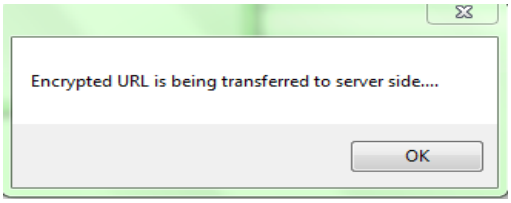

Figure 8. Transfer URL to DNS Server

Decryption of URL request

The DNS server decrypt the URL request and then send the user to that particular website and because this process takes few second the phishers are not able to hack the user information by spoof the fake DNS.

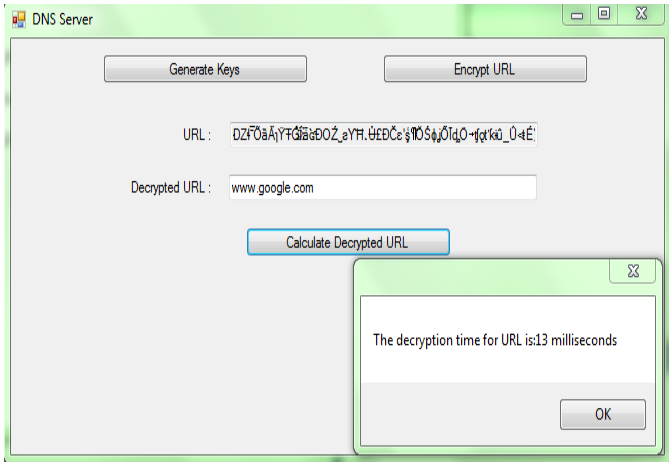

Figure 9. Decrypted URL

4. Testing

In the module we are test our work the proving that our authentication scheme will takes very less amount of time to execute because of which the attacker cannot able to spoof the fake DNS server within that execution time and failed to do any malicious activities we have used "ETTERCAP" network analyzer for spoof a fake DNS server. Ettercap is an open source tool that can set up Man-in-the-Middle attacks. It runs on different operating systems such that BSD, Linux, Windows and Mac OS X. ETTERCAP can capture passwords, sniff network traffic, *etc*.

ETTERCAP involves four modules:

- ***MAC-based:*** Filtered packets by MAC address.
- ***IP-based:*** Filtered packets by IP address.
- ***ARP-based:*** It is very useful for sniffing packets between two hosts on a switched network.
- ***Public ARP-based:*** It is very useful for sniffing packets from user to all hosts.

Important features of "ETTERCAP" are:

- OS fingerprinting
- Hijacking DNS
- HTTPS support
- Passive scanning

Activating DNS spoof plugin

For activate DNS spoof plugin we start up the ettercap NG-0.7.3 window 32 platform.

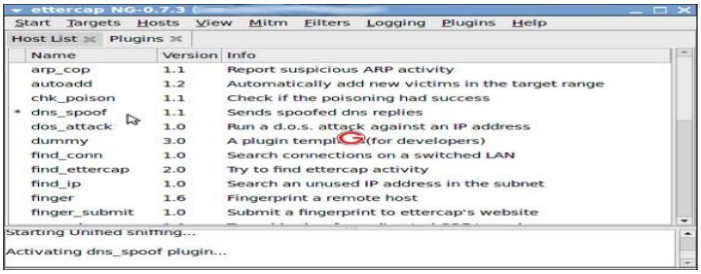

Figure 10. Activating DNS Spoof Plugin

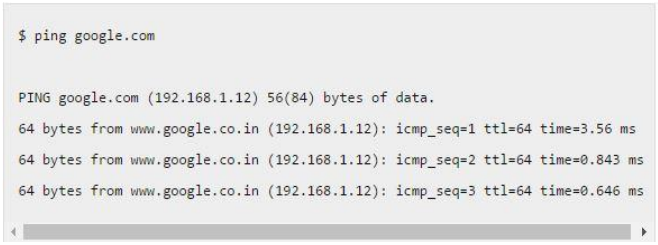

Figure 11. Ping Google.com

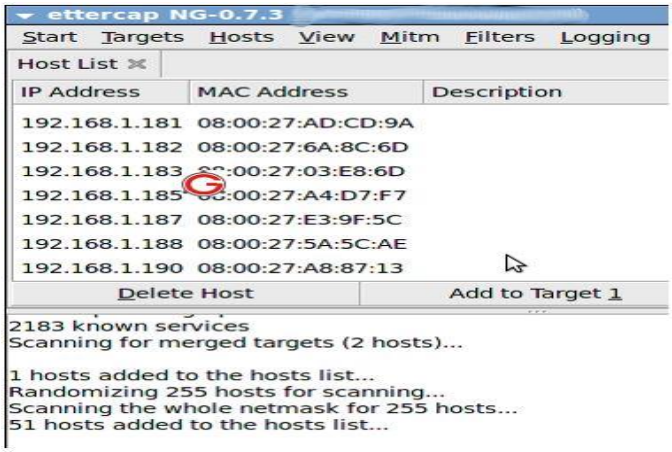

Figure 12. Scan Number of Host

This process is taking more time than our authentication scheme so its proved that our scheme can prevent the DNS sever by DNS spoofing and also protect the user to phishing attacks.

5. Related Work

There are several prior techniques have been proposed for prevention of DNS sever to isolate phishing attacks and avoiding DNS spoofing but in our work we used 64-bit public key encryption with time synchronizing mechanism that's why our work provides security in very few seconds before a fake user can spoof fake DNS server and phishing the user information .

"Redirecting Network Traffic toward a Fake DNS Server on a LAN" shows a new DNS attack that hack DNS requests by often times spoofing fake DNS server, and then the network systems communicates with fake destinations. The switch will be confused by duplicating MAC address and the IP and keep sending ping request to the switch by the attacker and as a result, it transmit the information to both ports that are connected to the real host and attacker's system .This type of attack is measurable by neither the IDS nor any anti spoofing software[2].

The [3] proposed that Phishing is a basic problem for exemplifying usable concerns of security and privacy because both attackers and system designers fight using user interfaces to guide users. They propose a new scheme titled "Dynamic Security Skins", that precluded a remote web server to demonstrate its identity in such a way that is easy for an authorized user to verify and hard for an attacker to spoof.

"PhishCatch – A Phishing Detection Tool". In this they developed a PhishCatch algorithm to probing phishing attacks. The Phishcatch algorithm is a heuristic program based algorithm which will identify phishing emails and warn the users about them. The phishing filters and regulations in the algorithm are designed after research of phishing methodologies. Testing module prove that Phish Catch algorithm has a catch rate of 80% and an accuracy of 99% [4].

6. Conclusions

DNS is the most vital components of the Internet basic structure, but is unguarded to spoofing. The main purpose of this paper is that to provide a security mechanism which protects the internet surfer to phishers and unknowingly access the unauthorized website. Each DNS user requires to obtain a unique key for access the DNS server and Server identify the authorized user by decrypt that key. Main feature of our work is time synchronization because of that it can able to response in few seconds and that's why

attacker is unable to do any malicious activities. Our work can also be used in confidential areas like banking sector and military areas and In future we will enhance the capability of access this mechanism lesser time period and try to implement our project in less number of bit encryption.

References

[1] Cryptography, Book Data communications and networking Fourth Edition Behrouz A. Forouzan DeAnza.
[2] M. Janbeglou, S. Ibrahim and M. Zamani, "Redirecting Network Traffic toward a Fake DNS Server on a LAN", 978-1-4244-5539-3/10/$26.00©2010IEEE.
[3] R. Dhamija and J. D. Tygar, "The Battle Against Phishing: Dynamic Security Skins", Proceedings of the 2005 ACM Symposium on Usable Security and Privacy, ACM International Conference Proceedings Series, ACM Press, **(2005)** July, pp. 77-88.
[4] Weider D. Yu Shruti Nargundkar Nagapriya Tiruthani (2009), "PhishCatch - A Phishing Detection Tool", 33rd Annual IEEE International Computer Software and Applications Conference, Computer Engineering Department, San Jose State University San Jose (Silicon Valley), California, USA 95192-0180.
[5] Center, S.I.S.: DNS cache poisoning update 7.4, **(2005)**.
[6] P. Likarish and E. (EJ) Jung, D. Dunbar and T. E. Hansen (2008), "B-APT, a Bayesian Anti-Phishing Toolbar", IEEE Communications Society, Dept of Information Science and Dept. of Computer Science The University of Iowa, Iowa City, Iowa 52246
[7] S. Abu-Nimeh and S. Nair (2008), "Bypassing Security Toolbars and Phishing Filters via DNS Poisoning", IEEE Communications Society subject matter experts for publication in the IEEE "GLOBECOM".
[8] P. Prakash, R. R. Kompella, M. Kumar and M. Gupta (2010), "PhishNet: Predictive Blacklisting to Detect Phishing Attacks", Mini-Conference at IEEE INFOCOM.
[9] U. Steinho, A. Wiesmaier and R. Araújo, "The State of the Art in DNS Spoofing", Department of Cryptography and Computer algebra Technische Universität Darmstadt Hochschulstr. 10; D-64283 Darmstadt, Germany.
[10] T. Chomsiri (2008), "Sniffing Packets on LAN without ARP Spoofing", X 978-0-7695-3407-7/08 $25.00 © 2008 IEEE DOI 10.1109/ICCIT.2008.318 Third 2008 International Conference on Convergence and Hybrid Information Technology.
[11] A. Tsow, School of Informatics Indiana University, "Phishing with Consumer Electronics: Malicious Home Routers".
[12] Fanglu Guo Jiawu Chen Tzi-cker Chiueh, "Spoof Detection for Preventing DoS Attacks against DNS Servers".
[13] M. Jakobsson and A. Young, "Distributed Phishing Attacks", School of Informatics, Indiana University at Bloomington, Bloomington, IN 47406. www.markus.jakobsson.com, LECG LLC, Washington DC, adamy@acm.org.

