iJRASET
International Journal For Research in
Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 6 Issue: I Month of publication: January 2018

DOI: http://doi.org/10.22214/ijraset.2018.1471

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor :6.887
Volume 6 Issue I, January 2018- Available at www.ijraset.com

Isolate Phishing Attacks by Preventing Domain Name Server Spoofing

Vikas[1]
[1]*Department of Computer Science and Engineering, GIMET (PTU Regional Campus), Amritsar*

Abstract: Phishing is an internet scam done by Web criminals. It harms the user's confidentiality through Phished Websites. DNS spoofing is also involved in Phishing in which attackers spoof the data by mimicking the original Website. DNS spoofing can inject Fake DNS server in place of original server and user directly redirect to a fake server and server get User's passwords and credit card numbers which is harmful for user data. In our research, we are preventing the DNS server from DNS spoofing. In our work, we have developed a robust algorithm that is combination of (RSA + bit stuffing), i.e. RSA accounts for legacy of user by providing the Digital signature, while bit stuffing is used digesting the message so that it remain confidential for the intruders, if any changes persists (violation of integrity) destination can't decipher the message with the help of public key of sender. So this way we can provide more robustness for DNS.

***Keywords:* Phishing Attack, DNS Spoofing, RSA Algorithm, Digital Signature, DNS Security.**

I. INTRODUCTION

The computer network is used in everyday life to conduct transactions, communications among businesses and folks. The protection afforded to an automated information system in order to attain the applicable objectives of preserving the CIA security of information system resources such as hardware, firmware, information data and telecommunications. Network security involves all activities that Organizations and Institutions embark to protect the value and ongoing usability of assets and the truthfulness and stability of operation. A valuable network protection approach requires identify threats and then choosing the most effective set of tools to combat them. Phishing attacks combine technology and social engineering to gain access to restricted information. Phishing is an internet scam where the user is convinced to give valuable information such as user name, passwords, credit cards secret information etc., from native user for impersonation attack and other fraudulent activities. Phishing will redirect the user to a different website through email, instant messages etc. A special kind of attackers provides clone malicious websites to the user to fill personal information. Fake websites which appear very similar to the genuine website are being hosted to achieve this and users think that they are entering their information into original website without realizing that they giving away their confidential information to a stranger who can misuse it for financial gain. The main purpose of phishing is to spoof the user's confidential information in other credentials like bank accounts. Phishing attacks can target audience through mass-mailing millions of email addresses around the world.In DNS spoofing data is introduced into a Domain name system name server's cache database, causing the name server to return a wrong IP address, diverting traffic to attacker's computer because of the open and distributed design of the DNS therefore it is vulnerable to various forms of attack. DNS spoofing is a term used when a DNS server accepts and uses incorrect information from a host that has no authority giving that data. DNS spoofing is essentially malicious cache poisoning where forged data is placed in the cache of the DNS. Spoofing attacks can be the origin of serious security problems for DNS servers susceptible to these kinds of attacks.

II. PROBLEM FORMULATION

Phishing attack is the most common attack of web applications. Phishing website is designed by the attacker and makes a fake page but they cannot send the fake link to legitimate website so attackers forced the legitimate user to open the link with the help of DNS spoofing. The original design of the Domain Name System (DNS) did not include security instead it was designed to be a scalable distributed system. DNS spoofing attack is an active attack and causes very serious problem and misuse the user confidential information. In Fig.1, DNS spoofing, attackers inject the fake DNS server by modifying the IP address. Now user does not know about fake DNS server. 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. Fake DNS hack all personal information of user and can use this information for illegal purpose.

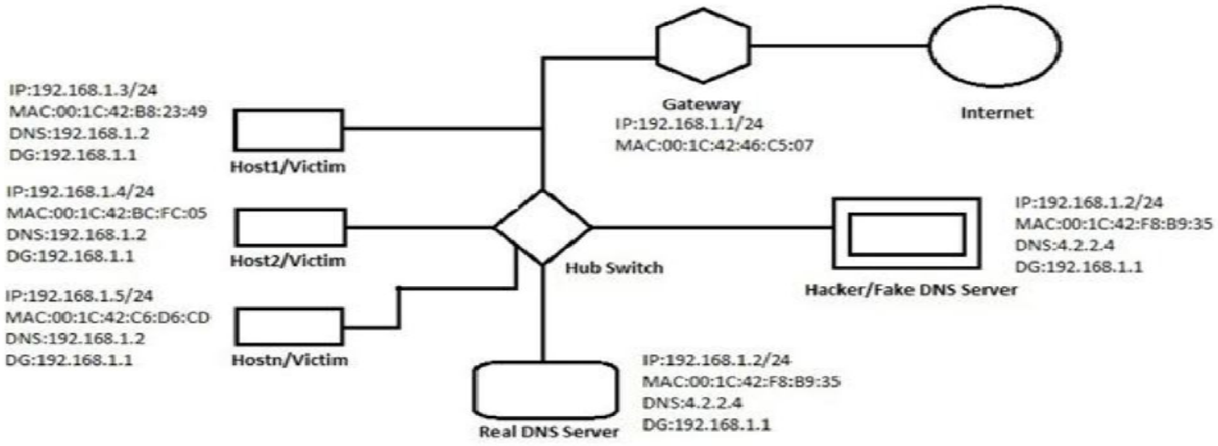

Fig. 1 Capturing network packets by hacker

In Fig. 2, clients will receive incorrect IP and consequently they will communicate with wrong destinations. These destinations might be fake web servers to gain username/password or private information of clients. Websites contain malicious content such as worms and viruses; fake update server for the software and operating system, and sometime it threatens the network availability.

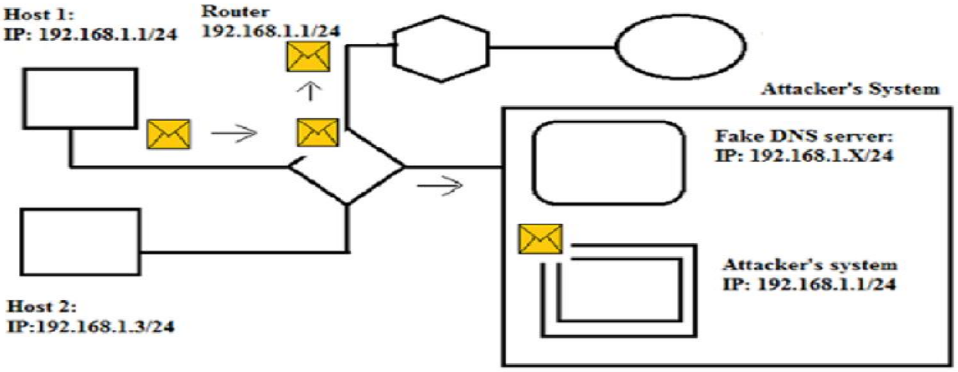

Fig. 2 Redirecting and responding Domain Name Server requests by the hacker

If we prevent DNS spoofing then phishing attack can be isolated so we are working to prevent DNS spoofing by adding DNS security extension.

III.PROPOSED TECHNIQUE

In Our technique We are preventing the DNS server from DNS spoofing. We havedeveloped a robust algorithm that is combination of (RSA + bit stuffing), i.e. RSA accounts for legacy of user by providing the Digital signature, while bit stuffing is used digesting the message so that it remain confidential for the intruders, if any changes persists (violation of integrity) destination can't decipher the message with the help of public key of sender. So this way we can provide more robustness for Domain Name Server.DNS spoofing attack is an active attack and causes very serious problem and misuse the user confidential information. If we prevent DNS spoofing then phishing attack can be isolated so we are working to prevent DNS spoofing. Phishing attack is possible through DNS spoofing. With the help of DNS spoofing, attacker can inject a fake server and change the IP address. When user try to redirect a webpage then he directly redirect to fake server and phished website automatically open and user giving him confidential data and attackers get user credentials and can misuse it. The idea behind this technique is to modify the RSA key from 512 bits to 512 bits by applying BIT STUFFING instead of ordinary integers using the same prime numbers used by the 512 bits. In this way we are making DNS more secure by using 512 bits and 512 bits for prime numbers. Confidentiality is the second function used in DNS. For the purpose of making message secure, We are using BIT STUFFING technique that will take care of message confidentiality because with the help of bit stuffing we padded message to maintain a fixed length. An arbitrary length of message is digested into fixed length message; active intruder can't decrypt it until they have knowledge about the padding bit added into arbitrary length input message. The RSA algorithm has been modified from the domain of integers to the domain BIT STUFFING. It was proposed that this modification is reliable and more secure than the classical RSA. So this way we can provide more robustness for DNS.

IV. METHODOLOGY USED

To Prevent the DNS Server from DNS Spoofing, We have developed a robust algorithm that is combination of (RSA + bit stuffing), i.e. R.S.A accounts for legacy of user by the Digital signature, while bit stuffing will be used digesting the message that it remain confidential for the intruders, if any changes persists (violation of integrity) destination can't decipher the message with the help of public key of sender. So this way we can provide more robustness for DNS. The methodology of our proposed work is given below:

A. Phase 1

Firstly We have developed the code for modified version of RSA Algorithm with Bit Stuffing using .Net Programming Language (C#) for user authentication while client/server communication as protocol. We have modified the RSA key from 512 bits to 512 bits by applying BIT STUFFING instead of ordinary integers using the same prime numbers used by the 512 bits. In this way We are making DNS more secure by using 512 bits and 512 bits for prime numbers. Confidentiality is the second function used in DNS.

B. Phase 2

We have developed the code for generating asymmetric keys (public+private) at server end using .Net Programming Language (C#). Public key is broadcasted by server to the user end. Public key keep secret for decryption purpose.

C. Phase 3

For client side encryption scenario, We have developed a code for providing Graphical user interface to client for encrypt any URL using server public key.

D. Phase 4

For server side decryption scenario, We have developed a code for providing graphical user interface at server for decrypt the URL received from client (encrypted url is a result of public key encryption + RSA algorithm + bit stuffing). Encrypted URL will be decrypted by server with its own private key and finally We got the decrypted URL.

E. Phase 5

We have implemented the complete proposed system scenario as Graphical implementation using Network Simulator 2 (NS2).

V. CONCLUSION AND FUTURE SCOPE

DNS spoofing is really concern in the aspect of security as all the requests placed by user pass through DNS so the request should be reached to the desire destination without any undesirable constraints. So in this study We are proposing a robust approach that will prevent active intruders to do any unwanted (unauthenticated) changes. Proposed algorithm describes a generalized approach that works on public cryptosystem along with bit stuffing, public cryptosystem that accounts for authenticity and bit stuffing that deals with message confidentiality by digesting message from arbitrary length size to fixed length. This process overcomes the limitation of RFC 2535. We strongly believe that this process take care of DOS attach as well because it restrict number of request by filtering the packet if it doesn’t fulfil the desired SLA. For the future aspect we are looking forward to provide confidentiality as well using MAC algorithm.

REFERENCES

[1] J. S. Downs, M. B. Holbrook, and L. F. Cranor, “Decision strategies and susceptibility to phishing,” presented at the Symp.Usable Privacy and Security, Pittsburgh, PA, 2006.
[2] Markus Jakobsson, Adam Young "Distributed Phishing Attacks" School of Informatics, Indiana University at Bloomington, Bloomington, IN 47406.
[3] Pawan Prakash, Manish Kumar, Ramana Rao Kompella, Minaxi Gupta (2010) "PhishNet: Predictive Blacklisting to Detect Phishing Attacks", Mini-Conference at IEEE INFOCOM.
[4] 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
[5] Alex Tsow, School of Informatics Indiana University "Phishing with Consumer Electronics: Malicious Home Routers"
[6] Fanglu Guo Jiawu Chen Tzi-cker Chiueh "Spoof Detection for Preventing DoS Attacks against DNS Servers"
[7] http://www.phishtank.com
[8] http://technet.microsoft.com/en-us/library/cc959354.aspx