International Journal of Advance Research in Engineering, Science & Technology(IJAREST),
ISSN(O):2393-9877, ISSN(P): 2394-2444,
Volume 2,Issue 10, October -2015, Impact Factor: 2.125

Mitigation of DNS Attacks using SSL Protocol

Ms.Kalyani Madan Kinhekar(kalyanikinhekar900@gmail.com)

Ms.Neha Nandkumar Kulkarni(nehankulkarni777@gmail.com)

ABSTRACT

Domain Name System continues to be a nice target for hacker. The Domain Name Server (DNS) is widely implemented database system use through the Internet, providing Name Resolution between host name and internal protocol address. This thesis describes problems with the Domain Name System and one of its implementations that allow the abuse of name based authentication.We examine the weaknesses in the DNS and exploit a method to abuse the Domain Name System for system break. With the use of Secure Socket Layer (SSL) Protocol, we are trying to decrease the severeness of DNS attacks.We can use Enhanced RSA (ERSA)and El-Gamal algorithm together for provide high level data security.

Keywords-

Security,DNS attacks,SSL,Cryptography.

1. INTRODUCTION

Application Layer Services

Visualizing the mechanisms that enable communication across the network is made easier if we use the layered framework of theOpenSystem Inteconnection(OSI)model.The OSI model is a seven-layer model which is designed to help for explaining the flow of information from layer to layer. It provides the first step of getting data onto the network.It consists of protocols that focus on process-to-process communication across an IP network and provides a firm communication interface and end-user services.The application layer provides many services like-Simple Mail Transfer Protocol,File Transfer,Web surfing,Web chat,Email clients,Network data sharing,Virtual terminals,Various file and data operations.More than 15 protocols are used in the application layer,including File Transfer Protocol, Telnet, Trivial File Transfer Protocol, Simple Network Management Management Protocol. Domain Name System(DNS) is also used to resolve Internet names to IP addresses. Application Layer used for making provisions for applications and services.

2. DNS INTRODUCTION

DNS, which stands for Domain Name System which controls your domain name's website and email settings. When visitors go to your domain name, its DNS settings control which company's server it reaches out to. It is a hierarchical distributed naming system for computers, services, or any resource connected to the Internet or a private network. It is an essential component of the functionality of most Internet services because it is the Internet's primary directory service.An often used analogy to explain the DNS is that it serves as the phone book for the Internet by translating human-friendly computer hostnames into IP addresses.Paul Mockapetris designed the Domain Name System at the University of California,Irvine in 1983,and wrote the first implementation at the request of Jon Postel from ISI.

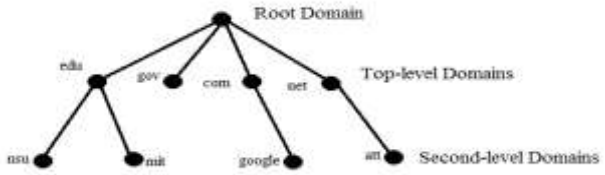
2.1 Name Resolution

When using the Internet most people connect to websites or other Internet servers by connecting to a domain name,as in www.gmail.com. Each web server has a unique IP address in textual form,translating it to an IP address,this process known as DNS resolution or DNS look.Most DNS server stores information like,hostname and their IP address,list of mail server and their IP address for given domain name,Anti spam cocontacts a DNS server that returns the translated IP address.nfiguration and much more.During the Dns resolution process,the program that wishes to perform the translation.When we type www.yahoo.com into a web browser,then application has to find out IP address associated with www.yahoo.com.

2.2 Hierarchical Structure of DNS

DNS uses a hierarchy to manage its distributes system of database.The DNS hierarchy,also calles domain name space,is an inverted tree structure.A period or dot(.) is the designation for root domain.Below the root domain are the top-level

domains which are divide the DNS hierarchy into segments.Within the hierarchy,start resolution form the top level domain,work your way down to the second-level domain,then through zero,one or more sub-domains until you get the actual host name you want to resolve into an IP address.



2.3 DNS Configuration

DNS allows the system to look up host names,both within the private network and across Internet.There are other way of doing this,for example,you could just run identical hosts file on all your machines.To configure Dns server,we need to set up a number of database files.The DNS server daemon first consults a Boot file.This boot file tells the daemon to consult a series of database files which gives it enough information to start serving names.Zone file of DNS is a text file that describes a DNS zone which is a subset of the hierarchical domain name structure of the DNS.Zone file contains the mapping between domain names and IP addresses and other resources ,organized in the form of text representations of resource records.If you want to override the default DNS settings on your computer,so you can specify which DNS server is used,or which IP address should be used for a particular domain.There are 2 ways to do it:Specify the DNS and map IP addresses.

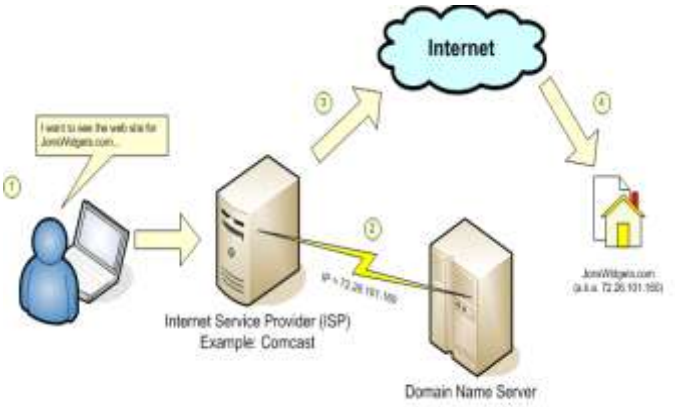
2.4 How DNS works

Without DNS,the Internet would be an ugly place.If you want to visit any website like www.gmail.com ,your browser needs to find the IP address of that particular web server.It conducts the system's hosts file,a text file with the IP addresses of any domain names that are effectively 'hard coded' into that system.If that web address is not in the system's hosts file,and this will almost always be the case,your browser will ask a DNS server-either resolver on your organization's network or an external,public resolver may be operated by an ISP or by organization like Google.If the resolver has recently asked for the IP address for that domain name,it will have that information in its cache and it will provide it directly.But if it has not got in its cache,then it will refer the request on to a root server,which can tell the resolver where to get information about the .com top-level domain.Then it will ask the server ,where to get information about

3. DoS Attacks/DDoS Attacks On DNS

DNS based attacks are on the rise because many organizations do not realize DNS is a threat vector and therefore do not protect it.In recent years,Denial of Service (DoS)attacks on DNS has a trend to be more serious problems.DDoS attack is a packet flood from thousands of computers across the Internet toward one server with the intent of its bandwidth and shutting it down to legitimate users.DoS are the common computer system attacks which main purpose makes a machine,service,system or other essential components of a computer system to be unavailable.Most DoS attacks employ the IP spoofing to conceal identities of attacking machines.DNS Spoofing or DNS Cache Poisoning is a computer hacking attack introduced into a DNS resolver's cache,causing the name server to return an incorrect IP address,diverting the traffic to the attacker's computer or any other computer.DDoS has taken place in following areas:preventing DDOS attacks through packet filtering,Intrusion tracing,foiling attacks aimed at the TCP protocol,limiting the rate of attack-packet flow at upstream routers,improving capabilities in detecting DDOS attacks.

gmail.com and then go to that server which is authoritative server,which will provide it with the IP addresses of any servers in the gmail.com domain.



3.1 How DNS attacks are solved

There have been many instances of flooding attacks on the DNS aimed at preventing clients from resolving records belonging to the zone under attack.DNS's pivotal role as a precursor to almost all Internet services implies that such attacks represent a severe threat to Internet in general.In response to such attacks,some DNS root-servers and top-level domain servers have been replicated through IP Anycast. For preventing DNS attacks,keep your resolver private and protected.Also configure it to be as secure as possible against cache poisoning and manage your

DNS servers securely because,no one cares about your security as much as you do.

3.2 Protocols for supporting mitigation of DNS attacks

Mitigation is a term employed to design the means and measures in place that reduces the negative effects of a DDoS attacks.The DNS protocol is an effective DoS attack vector for few reasons like DNS generally uses the connectionless UDP as its transport, many autonomous systems allow source-spoofed packets to enter their network,there is no shortage of open resolvers on the Internet.These three factors means that attackers can creat large amount of unwanted response packets by reflecting DNS queries.In such attacks,DNS query is generated with spoofed source IP addresses belonging to victim.Network Time Protocol(NTP) is used by machined connectes to the Internet to set their clocks accurately.A simple UDP-based NTP protocol is prone to amplification attacks because it will reply to a packet with a spoofed source IP address.The ASA,PIX and FWSM firewall products,Cisco Intrusion Prevention System(IPS) and Cisco IOS NetFlow feature,provide capabilities to aid in identification and mitigation for DNS related attacks.

4. Role of Secure Socket Layer(SSL) in mitigating DNS attacks

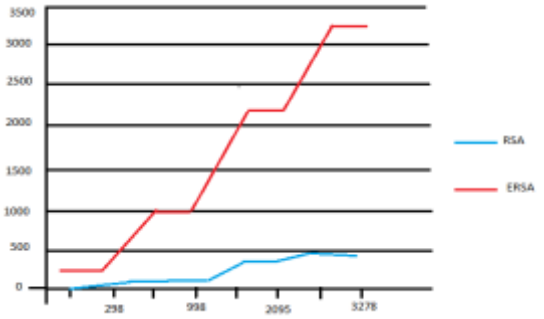
SSL is a standard security technology for establishing an encrypted link between a server and a client.SSL uses a cryptographic system which uses two keys for encryption of data-public key known to everyone and private or secret key known only to the recipient of the message.SSL protocol is used by millions of e-Business providers to protect their customers, ensuring their online transactions remain confidential.In SSL protocol, we can use Enhanced RSA on behalf of RSA algorithm.

RSA key is private key which is based on RSA algorithm used for authentication and symmetric key exchange during establishment of an SSL session.SSL uses both symmetric and asymmetric encryption.For that purpose,RSA algorithm is used. If we compare RSA with Enhanced RSA,timeof encryption,decryption,execution time of RSA is less than Enhanced RSA.And ERSA gives more security and confidentiality than RSA.The observed result is shown below-

File Size (Bytes)	Algorith--ms	Encryption Time(sec)	Decryption Time(sec)	Execution Time (sec)
298	RSA	23	3	26
	ERSA	20	2	22
998	RSA	65	7	72
	ERSA	62	6	68
2095	RSA	296	14	310
	ERSA	286	10	296
3278	RSA	397	17	414
	ERSA	358	13	371

The following diagram shows the execution time of algorithms-

File size is shown in X-axis and Execution time in Y-axis.



5. PROPOSED SYSTEM

SSL uses public key encryption technology for authentication. With public key encryption,a public key and private key are generated for a server.The keys are related for data encryption with public key,also it can be decrypted using the corresponding private key and vice versa.The private key is carefully protected so that only the owner can decrypt messages that were encrypted using the public key.We can mitigate the DNS attacks by using the SSL with the use of ERSA and El-Gamal algorithm.

5.1 Enhanced RSA:

We can merge both Enhanced RSA algorithm and Elgamal algorithm to provide user with the higher level of data security. The enhanced RSA algorithm enables faster encryption and decryption and generate public and private key faster than original RSA algorithm. We can generate three prime numbers instead of two prime numbers with reduce size which will generate variable N with large size.

Key Generation:- Choose three distinct prime numbers as p,q,s. Firstly,find n such that n=p*q*s.Let n be the modulus of both public and private key.Secondly,

Phi(n)=(p-1)(q-1)(s-1).Then,choose e such that, 1<e<Phi(n). e and Phi(n) share no division other than 1.e is the public key exponent. Determine(d) satisfies congruence relation D*e=1(mod Phi (n)).

5.2 Elgamal Algorithm:

This algorithm allowing for multiple valid signatures for a given message.The security depends on the difficulty of Discrete Log Problem. Firstly,find a large prime p, generator g of Z*p.Pick x belongs to Zp-1 which is the private key.Compute y=g^x(mod p)as a public key.Pick any random number k and Z*p-1.This makes Elgamal Non-deterministic. Then, generate signature. To verify the signature ,check y^a*a^b=g^M(mod p).

With the use of these merging of attacks, we can slightly mitigate the DNS attacks. Use of those algorithms with SSL makes your system more reliable. It is difficult for the attacker to attack on the system.

Time complexity analysis of proposed algorithm-

Message size	RSA	Enhanced RSA	Elgamal	RSA-Elgamal	Proposed Method
1KB	0.00326 Sec	0.00157 Sec	0.02697 Sec	0.00778 Sec	0.00678 Sec
2KB	0.00346 Sec	0.00323 Sec	0.03959 Sec	0.01428 Sec	0.03959 Sec
3KB	0.00479 Sec	0.00450 Sec	0.04763 Sec	0.02177 Sec	0.02046 Sec
4KB	0.00759 Sec	0.00724 Sec	0.05606 Sec	0.02867 Sec	0.02867 Sec
5KB	0.00829 Sec	0.00786 Sec	0.06758 Sec	0.03862 Sec	0.03422 Sec
10KB	0.01669 Sec	0.01532 Sec	0.12194 Sec	0.07409 Sec	0.07227 Sec
20KB	0.0031865ec	0.003122 Sec	0.23498 Sec	0.16017 Sec	0.15899 Sec
Average Time	0.01085 Sec	0.01013 Sec	0.06908 Sec	0.04934 Sec	0.04766 Sec
Throughput (Mega Bytes/Sec)	4.05069 Sec	4.33859 Sec	0.63622 Sec	0.89076 Sec	0.92216 Sec

6. REFERENCES

[1] "ERSA: Secure and Enhanced RSA"-V.Saravanakumar: International Journal of Engineering Research and Applications(IJERA)

[2] "A New Encryption Scheme Based on Enhanced RSA and El-Gamal"-Mini Malhotra-Department of Computer Science,Lovely Professional University,Punjab,India.

[3] M.Handley and A.Greenhalgh,"The Case For Pushing DNS".

[4] H.Ballani and P.Francis, "A Simple Approch to DNS Dos Mitigation," in proc.of workshop on Hot topics in Network,Nov 2006.