International Journal of Research
ISSN: 2348-6848 Vol-3, Special Issue-3
International Conference on Research and Recent Trends in Engineering and Technology. (ICRRTET)
Held on 27th January 2016 organized by **Sai Polytechnic College,** Kinhi Jawade, Yavatmal, Maharastra, India.

A Review on securing Domain Name System using Advanced Encryption Standard

Mr. Jayesh Shende; Miss.Asawari Kawle & Miss.Trupti Raut

ABSTRACT:
The mapping of IP addresses to host names is a major problem in rapidly growing internet. The higher level binding effort went on increasing to different level of development up to the currently used Domain Name System. DNS, being an open source, it is less secured and it has no means of determining whether domain name data comes from an authorized domain owner. So these vulnerabilities lead to a number of attacks. Hence, there is a need of securing DNS. Using Advanced Encryption Standards, it performs normal encryption. By reversing this encryption, decryption is also performed. Domain Name System has number of workgroups and these workgroups are connected to the server. This server is connected to the server of other domain and the proposed system secures client using AES.
Index Terms- DNS Security; public key infrastructure; AES.

INTRODUCTION

The name system (DNS) is web Directory Service. It's thought-about collectively of the fore most necessary components of the stylish web. A web site name is also a purposeful and easy-to-remember handle for science address. DNS is also a consumer server application that maps host names into their corresponding science address. DNS is that the foremost eminent largest distributed data so security for DNS is unbelievably necessary. It is important to secure DNS as a result of the suggests that of threat have accumulated presently Associate in Nursing excessive quantity of extent. The projected system uses the AES algorithm to have security against attack on the DNS. Advanced secret writing customary, is also a bilaterally interchangeable. Block cipher which will inscribe info blocks of 128 bits exploitation symmetric keys 128, 192, or 256. AES inscribe the data blocks of 128 bits in 10, twelve and fourteen spherical counting on the key size. Half attacks that the entirely effective attack superb against this recursive.

In pc networking, a packet drop attack or part attack could be a style of denial-of-service attack within which a router that's imagined to relay packets instead discards them. This typically happens from a router changing into compromised from variety of various causes. One cause mentioned in analysis is through a denial-of-service attack on the router employing a better known DoS tool. As a result of packet square measure habitually born from a loss network, the packet drop attack is extremely exhausting to find and forestall. The malicious router can also accomplish this task by selection, eg. By dropping packets for a specific network destination, at an explicit time of the day, a packet each n packet or each t second or at random hand-picked portion of the packets. This can be rather referred to as a gray-hole attack. If the malicious router tries to drop all packets that are available in, the attack will really be discovered fairly quickly through common networking tools like trace route. Also, once different router notice that the comprised networking like trace out. Also, once different routers notice that the comprised router is dropping all traffic typically will flow to the attack. However, if the malicious router begins dropping packet on a particular period or over each n packet, it's typically more durable to find as a result of some traffic still flows across the network.

The packet drop attack is often of times deployed to attack wireless unexpected networks. As a result of wireless networks have a far completely different design than that of a typical wired network, a number will broad cast that it's the shortest path towards a destination. By doing this, all traffic is directed to the host that has been compromised, and also the host is ready to drop packets at can. Conjointly over a mobile unexpected network, host square measure specifically prone to cooperative attacks wherever multiple hosts can become comprised and deceive the opposite hosts on the network.

OVERVIEW OF DNS

As already mentioned DNS may be a world, stratified and distributed information. This information associates names that are unit said as domain names, with bound knowledge contained in resource records (RRs). Records coupled to a website name will be of regardful sorts, however the address sort is that the most typical one. There will be multiple RRs of identical sort for one name. The set of resource records of identical sort is named a resource record set (RRset). Since domain name go to be globally distinctive, a stratified naming theme is employed. A website name refers to a node during a tree that is named the name area. This tree of domain name is incredibly just like the structure of an operating system beer system. Every sub tree is named a website. For instance, the sub tree non-moving on the .com node is named the .com domain and includes all domain ending with .com The nodes that area unit directs kids of the foundation node area unit referred to as high level domains. Communication with the DNS information follows the client/server paradigm.The name tree is into zones, that sometimes area unit contiguous components of the tree. Zones area unit outlined by the method of delegation that signs to some organization the responsibility of managing specific subdomains. A zone could contain info a few domain and its sub domains. Commanding zones, such as .edu would largely contain delegation info. Foe every zone, there are a unit authorities server's respondent all queries regarding domain names their zone. Name server will be authorities for multiple zones, too.

A DNS consumer program is named a resolver. There are 2 varieties of resolvers: real resolvers and stub resolvers are essentially a library that must be put on in each host that wishes to access the DNS information. On every occasion a question a question must be sent, functions of this library are known as and therefore he method of retrieving the specified data is run. Specially, the stub resolver usually settled on a DNS server and serves a bunch of stub resolvers. Once an algorithm question is received, the resolver typically sends associate degree unvarying question to 1 of the basis DNS server serving the basis domain. Unvarying queries able a DNS server, that doesn't have the requested mapping to point consecutive server within the chain that is\ closer to the authoritative server for those queries. Within the example in, the resolver cesium.jhu.edu receives an algorithmic question for the information science address of the server web.lab.com from host's ho1.cs.jhu.edu. The resolver then sends associate degree unvarying question to a root DNS server that returns the information science address of the DNS server authoritative for the.com zone. The resolver can then question the name for laboratory.com. Finally, the DNS server of laboratory.com is queried by the resolver and returns the information science address of web.lab.com that's authoritative. This answer is then forwarded by the resolver to the stub resolver ho1.cs.jhu.edu. The whole method is named resolution. Root servers are essential to the practicality of the DNS system. There are presently thirteen root DNS seer distributed everywhere the world. Caching techniques are utilizes to cut back the amount of requests so as to hurry up th resolution method and to cut back networks utilizes cut back the amount of rquests so as to hurry up the resolution method and to cut back network traffic. Consequently, every RR that's came back from a DNS server encompasses a bound time-to-live that is that the time the RR is cached.

LITERATURE REVIEW

The DNS was designed as a replacement for the older "host table" system. Each were supposedto produce names for network resources at an additional abstract level than network (IP) addresses (see, e.g.,[RFC625], [RFC811], [RFC819], [RFC830], [RFC882]). In recent years, the DNS has become info of convenience for the net, with several proposals to feature newoptions. Just some of those proposals are no-hit. Usually the most motivation for victimizationthe DNS is as a result of it exists and is wide deployed, not as a result of its existing structure, facilities, and content area unit acceptable for the actual application of knowledge concerned. This document reviews the history of the DNS, together with examination of a number of those newer applications. It then argues that the overloading method is commonly inappropriate. Instead, it suggests that the

DNS ought to be supplemented by systems higher matched to thesupposed applications and descriptions a framework and explanation for one such system. To attach to a system that supports information science, the host initiating the association shouldunderstand ahead the informati on science address of the remote system. An information science address could be a 32-bit range that represents the situation of the system on a network. The 32-bit address is separated into four octets and every octet is usually described by a decimal range.The four decimal numbers are unit separated from one another by a dot character. Even if four decimal numbers could also be easier to recollect 32 1's and 0's, like phone numbers, there's a sensible limit on what percentage information science addresses an individual will keep in mind while not the necessity for a few type of directory help. The directory basically assigns host names to information science address. The standard analysis Institute's Network Info Centre became to accountable authority for maintaining distinctive host names for the net. The SRI-NIC maintained one file, referred to as hosts.txt and sites would unceasingly update SRI-NIC with their host name to information science address mapping to feature to, delete from, or amendment within the file. The matter was that because the web grew speedily, thus did the file inflicting it to become progressively tough to manage. Moreover, the host names required to be distinctive throughout the worldwide web. With the growing necessity for such things as a hierarchal naming structure and distributed management of host names sealed the means for the creation of a replacement networking protocol that was versatile enough to be used on a world scale.

What evolved from this can be online distributed that maps the names of laptop system to their individual numerical information science network addresses. This net operation facility is that the DNS. Necessary to the construct of the distributed information is delegation of authority. Now not is one single organization to blame for host name to information science address mappings, however rather those sites that square measure to blame for maintaining host names for his or her organizations will currently regain that management.

FUNDAMENTALS OF DNS

The DNS not solely supports host names to network address resolution, referred to as forward to as forward resolution; however it additionally supports network address to host names resolution, referred to as inverse resolution. Attributable to its ability to map human unforgettable system names into electronic network numerical addresses, its distributed nature, and its lustiness, the DNS has evolved into an essential part of the web. Without it, the sole thanks to reach different computers on the web is to use the numerical network address. Exploitation scientific discipline addresses to attach to remote system isn't an awfully easy illustration of a system's location on the web associated therefore the DNS is heavily relied upon to retrieve an scientific discipline address by simply referencing a pc system's absolutely Qualified name(FQDN). A FQDN is largely a DNS host name and it represents wherever to resolve this hostname at intervals the DNS hierarchy.

PROBLEM FORMULATION

Original DNS specifications failed to embody security supported the actual fact that the data that it contains, specifically host names and information processing addresses, is employed as a method of communication knowledge. As additional and additional information processing based mostly application developed, the trend for victimization information processing addresses and host names as a basis for permitting or disallowing access grew. UNIX operating system saw the arrival of Berkeley "r" commands and their dependencies on host names for authentication. Then several alternatives protocol evolved with similar dependencies, like Network classification system, X windows, machine-readable text Transfer Protocol. Another causative issue to the vulnerabilities within the DNS is that the DNS is intended to be a public formation during which the thought of proscribing access to among the DNS name house is intentionally not a part of of the protocol. Later versions of the BIND implementation permit access controls for such things as zone transfers, however beat all, the thought of proscribing United Nation agency will question for the DNS for RRs is taken into account outside the scope of the

protocol. The existence and widespread use of such protocols because the r-commands place demands on the accuracy of data contained within the DNS. False data among the DNS will cause sudden and probably dangerous exposures. The bulk of the weakness among the DNS be one in every of the subsequent categories: Dead Addresses, Firewall and "stealth" ports, part Filtering, DNSBL and compromise of the DNS server's authoritative knowledge.

1) **Dead Addresses-**

The most common form of black hole is simply an IP address that specifies a host machine that is not running or an address to which no host has been assigned. Even though TCP/IP provides means of communicating the delivery failure back to the sender via ICMP, traffic destined for such addresses is often just dropped. A dead address will be undetectable only to protocols that are both connectionless and unreliable (e.g., UDP). Connection-oriented or reliable protocols (TCP, RUDP) will either fail to connect to a dead address or will fail to receive expected acknowledgements.

2) **Firewalls and "stealth" ports-**

Most firewalls can be configured to silently discard packets addressed to forbidden hosts or ports, resulting in small or large "black holes" in the network. Personal firewalls that do not respond to ICMP echo requests have been designated by some vendorsas being in "stealth mode". Despite this, in most networks the IP addresses of hosts with firewalls configured in this way are easily distinguished from invalid or unreachable IP addresses. On encountering the latter, a router will generally respond with an ICMP network ISP host unreachable error. NAT, as used in home and office routers, is generally a more effective way of obscuring the layout of an internal network.

3) Black hole filtering

Black hole filtering refers specifically to dropping packets at the routing level, usually using a routing protocol to implement the filtering on several routers at once, often dynamically to respond quickly to distributed denial-of-service attacks.

4) DNSBL

A DNS-based Black hole List (DNSBL) or Real-time Black hole List (RBL) is a list of IP addresses published through the Internet Domain Name System either as a zone file that can be used by DNS server software, or as a live DNS zone that can be queried in real-time. DNSBLs are most often used to publish the addresses of computers or networks linked to spamming; most mail server software can be configured to reject or flag messages which have been sent from a site listed on one or more such lists. The term "Black hole List" is sometimes interchanged with the term "blacklist" and "block list".

A DNSBL is a software mechanism, rather than a specific list or policy. There are dozens of DNSBLs in existence, which use a wide array of criteria for listing and delisting of addresses. These may include listing the addresses of zombie computers or other machines being used to send spam, listing the addresses of ISPs who willingly host spammers, or listing addresses which have sent spam to a honeypot system.

Since the creation of the first DNSBL in 1997, the operation and policies of these lists have been frequently controversial, both in Internet advocacy and occasionally in lawsuits. Many email systems operators and users consider DNSBLs a valuable tool to share information about sources of spam, but others including some prominent Internet activists have objected to them as a form of censorship. In addition, a small number of DNSBL operators have been the target of lawsuits filed by spammers seeking to have the lists shut down altogether.

Symmetric key algorithm is algorithm for cryptography that uses same key for encryption and decryption. Encryption of plain text and decryption of cipher text is done. AES is reversible this means that almost the same steps are performed to complete both encryption and decryption in reverse order. The AES algorithm operates on bytes, which makes it simpler to implement and explain.

The client of one domain communicates with client of other domain using a packet as the medium. If the data contains malicious code then Black Hole attack occurs on the client. The data will not be received and the packet will be dropped. Here, AES is implemented on the server of domain where attack occurs. It is provided on the client of the same domain. In networking, black holes refer to places in the network where incoming or outgoing traffic is

silently discarded i.e., dropped without informing the source that the data did not reach its intended recipient.

On the other hand, if the packets have general data that is free from malicious code will be sent to the receiver client successfully.

PROPOSED SYSTEM

The proposed system uses the AES algorithm to have security against attack on the DNS. Advanced Encryption Standard, is a symmetric block cipher that can encrypt data blocks of 128 bits using symmetric keys 128, 192, or 256. AES encrypt the data blocks of 128 bits in 10, 12 and 14 round depending on the key size. Black Hole attack is the only effective attack known against this algorithm. Each time the System get the message, it verifies the IP Address of the sender and if no match is found it discards it. For verification, the Destination System generates Signature using Public Key and AES Algorithm and verifies it with received one. If it matches it Decrypts otherwise it discards. The Following functions avoids the pitfalls of the existing system

- Fast and economical system.
- Simple access to system.
- Manual effort is reduced.

CONCLUSION

The widespread use of DNS and its ability to resolve host name to IP address for each users and applications alike during a timely and fairly reliable manner makes it important part of the net. But the first DNS protocol specification didn't embrace security. While not security, the DNS is at risk of attack. The area unit varied security measures adopted in DNS mistreatment isobilateral key cryptography, which incorporates AES. With the technology growing day by day, there's necessity of same level of security with giant block sizes. The planned system so aims at providing security against the region attack on DNS mistreatment Advanced Coding rule.

REFERENCE

[1] Giuseppe Ateniese, Stefan Mangard "A New Approach to DNS Security (DNSSEC)" IN CCS'01, November 5-8, 2001, Philadelphia, Pennsylvania, USA.

[2] Sachin Kumar Sinha, Avinash Kant Singh, Amaresh Sharma "Security System for DNS using Cryptography" International Journal of Engineering Research & Technology (IJERT)Vol. 2 Issue 2, February- 2013.

[3] PaulAlbitz,Cricket Liu, "DNS and BIND", Third Edition, O'Reilly, Sebastopol, CA, 1998, ISBN 1-56592-512-2, pp83-89,207.

[4] D.Atkins and R. Austein, "Threat Analysis of the Domain Name System (DNS)",RFC 3833, August 2004.

[5] P.Mockapetris, "Domain Names –Concepts and Facilities", STD special Publication s13,RFC 1034, November 1987.

[6] S. Rose and A. Nakassis, "Minimizing Information Leakage in the DNS", IEEE Network Magazine vol. 22 no. 22 April 2008.

[7] R. Arends, R. Austin, M. Larson, D. Massey, and S. Rose, "DNS Security Introduction and Requirements", RFC 4033, March 2005.

[8] B. Laurie, G. Sisson, R. Arends and D. Blacka, "DNS Security (DNSSEC) Hashed Authenticated Denial of Existence", RFC 5155, March.