3rd National Conference on Green Technology and Science for Sustainable Development
© 2020 IJSRST | Volume 5 | Issue 6 | Print ISSN: 2395-6011 | Online ISSN: 2395-602X
International Journal of Scientific Research in Science and Technology

An Efficient Implementation of Digital Signature Algorithm with SRNN Public Key Cryptography

Nisha Keshpage, Mohini Morey
Department of Information Technology, Anuradha Engineering College, Chikhli, Maharashtra, India

ABSTRACT

A digital Signature Algorithm verify the undivided of the signed data and the recognize of the signature. Cryptographic protocols provide services like entity authenticated key transport and authenticated key agreement. This architecture is connected with secure Hash Function and 512-bit SRNN cryptographic algorithm. SRNN cryptographic algorithm is based on RSA algorithm with some modification. SRNN algorithm is include more security .1n this algorithm we have an extremely large number increased the security of cryptography system. In this paper, a new algorithm has been designed for generation signature that overcomes the short coming of the RSA system. The new algorithm can be achieving high security. The security of DNS is paramount case DNS infrastructure is vulnerable and compromised, organization lose their revenue, they face downtime, customer dissatisfaction, privacy loss, confront legal challenges and many more. As we know that DNS is now become the biggest disposed database, but initially at the time of DNS design the only goal was to supply climbed and available name resolution service but its security perspectives were not focused and overlooked at there is an urgent requirement to provide some additional mechanism for addressing known vulnerabilities.

Keywords : Public Key Cryptography, Digital Signature, RSA, SRNN.

I. INTRODUCTION

The Domain Name System is the origination of internet which translates user friendly named based Resource Records (RR) into corresponding IP addresses and vice-versa. But nowadays DNS is not only addresses interpreting is more than this to provide authentication and improve security services of many internet applications. Now DNS becomes most vital part of internet and it should work properly other than whole internet communication will collapse. Therefore security of DNS fundament is one of the core requirements for any organization. In the present situation the applications like ecommerce and secure communications over open networks have But, the problem that goes with these solutions is that the private keys need to be secured in these applications. This problem is further worsened in the cases where a single and unchanged private key has to be kept secret for very long duration (such is the case of certification authority keys, and e-cash keys). Digital signatures are used to detect unacceptable modifications to data and to verify the identity of the signature.

II. DNS FUNCTION

Before discussing the security challenges of DNS, we need to understand the DNS functionality. Hosts

request for a particular resource by sending a ”recursive” query to its configured DNS Servers. Clients will get the name resolution answer of forwarded query or error message that it could not found anywhere. As we have discussed DNS servers are distributed globally, so before giving error message they query other name servers until it gets the answer or query failed response. so, basically DNS their queries and they are not configured with any administrative controls. Open resolver is a hot cake for attackers and can be vulnerable to perform following malicious activities and attacks against DNS servers.

• DoS or DDoS attacks

DDoS attacks can have a authoritative impact on the global DNS database and its users. They are usually directed at root servers. This was apparent with the recent DDoS attack in June 2004 [28], which was a repeat of a similar attack in October 2002 [20]. These attack caused a loss of availability of name resolution functions on two queries one is recursive and other is iterative. Queries which are initiated from clients are recursive queries and other search queries are iterative which are initiated from local DNS servers to authoritative receive query from clients and it doesn't have information in its cache, then they forward" DNS Referral Message" back to clients for the name server that may have the answer which can be authoritative name server or a lower level DNS in a hierarchical structure as we talked earlier. Figure below illustrates recursive and iterative queries used in DNS.

III. DNS VULNERABILITIES AND SECURITY CHALLENGES

The DNS flaws exist if DNS server will not configure properly. DNS or Name servers play a most critical role in overall internet communication. This service is being used on multiple platforms, operating systems, countless applications, various operators and technical experts. This must be hardened in order to avoid from its malicious threats and attacks. Most common flaws are mentioned in this document to inform DNS community how vulnerabilities can be exploited and DNS become vulnerable. Along with this best practices and techniques are also discussed in this paper to prevent these types of malicious activities.

IV. DNS VULNERABILITIES AND KNOWN ATTACKS

DNS Open Resolver DNS Open Resolver is DNS server which is open to all clients to provide name resolution regardless the requestor is part of its domain or not. So, they are entertaining requests (queries) to every client by responding them back to services to the internet community.

• DNS Cache Poisoning Attacks

DNS Cache Poisoning attacks [3] are very serious threat against DNS infrastructure. It's very easy idea to understand including a name server to cache bogus resource records where these bogus resource records might be machines or hosts run by hacker. For example bogus address for some.bank.com, or any insurance company's website poisoned with the IP address of webserver run by hacker where hackers hosted digitally identical replica of targeted original website and all users will be false victim to cache poisoning attack where end users are victimized for login, password, account info, credit card numbers are captured and so on will be recorded and used later on. Another example of cache poisoning attack is to falsify email communication with rerouting email by using poisoned MX record of hacker and then email may be modified without the sender knowledge. This attack introduces false information into DNS caches. This is undertaken by means of DNS RRs whose RDATA portion includes a DNS name which can be used as a hook to let an attacker feed bad data into a victim's cache. The most stirred types of RRs are CNAME, NS,

and DNAME RRs. False data, related with these names, can be injected into the victim's cache via the Additional section of the response. An Attacker can exhibit arbitrary DNS names of the attacker's choosing, and provide further information that is claimed to be associated with those names.

• Resource Utilizing Attacks

Resource Utilizing Attacks are used to degrade the performance of open DNS server by utilizing device resources like memory, CPU, socket buffers. These attacks will consume all available resources of open server and directly impact on the operations of open resolver and servers may have to stop or restart DNS services or may be reboot the server in order flush from occupied system resources

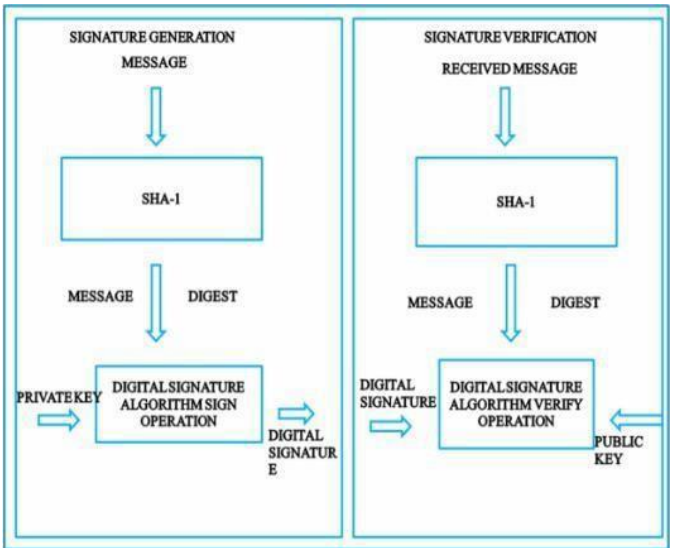

Fig 1: Digital Signature Scheme

V. RSA ALGORITHM ARCHITECTURE

For the RSA public-key cryptosystem mechanism, the design of Blakley [3] is used. Blakley introduced an algorithm in order to estimate the equation, P = A*B mod M. This algorithm is based on the repeats of one basic process until the beneficial calculation of product P. The transmitter wide of A, B, M, that is 5 12-bit in our case, defines the equal number of

VI. DIGITAL SIGNATURE ALGORITHM

A digital signature is symbolized in a computer as a string of binary digits. A digital signature is computed using a set of conditions and authenticates the alterness of the signed data also with the identity of the signature. An algorithm provides the applicable to generate and verify signature. Signature generation uses of a private key to produce a digital signature.Signature declaration uses of a public key, which compatible to, but is not the same as, the private key. Each user has a private and public key couplet. Public keys are known to the public in general and Private keys are never shared. Anyone can verify the signature of a user by using that user public key. Only the possessor of the user private key can perform signature propagations. Basically a hash function is used for signature procreation process to obtain a other version of data, known as message dispose (Figure I). The message dispose is then input to the digital signature algorithm to generate the digital signature and sent to the intended verifier along with the message after that the verifier of the message, signature verifies the signature by using the sender's public key. The same hash function must also be used in the confirmation process. The hash function is indicated in a separate standard, the Secure Hash Standard, FIPS 180 [2]. FIPS recommended digital signature algorithms must be mechanized with the Secure Hash Standard. Similar procedures may be used to decide and verify signatures for stored as well as transmitted data. The Digital Signature Standard (DSS) uses three algorithms for digital signature generation and verification. The Digital Signature Algorithm (DSA). THe algorithms repeats procedure. Fig. 3 shows the implemented RSA algorithm architecture. The RSACONFIG is used in order to store the system confirmed information. Include of two registers that are used for the storage of the negotiate plaintext and key. The control unit ensures

the correct information m ovements intermediate the units.

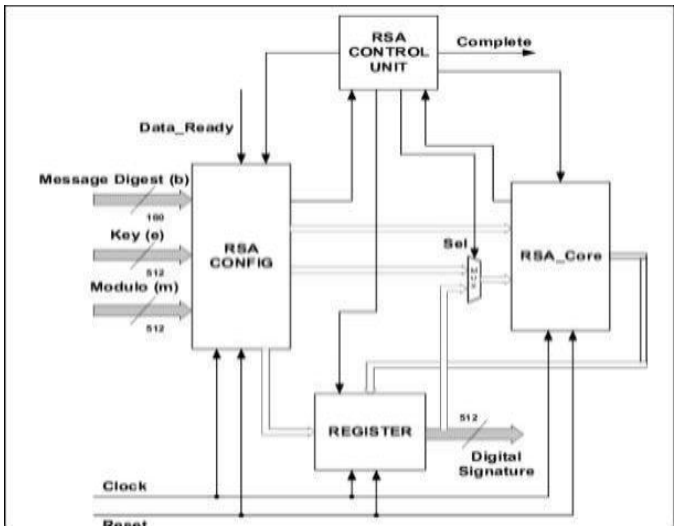

Fig 2. The RSA Algorithm Architecture

VII. CONCLUSION

In this paper SRNN algorithm is used for digital signature scheme with 512-bit SRNN algorithm behalf of this algorithm we can the secure the communication channel for sender and recipient. further algorithm we can use for (1024-bit) SRNN. In this algorithm and proposed signature generation, verification is more secure than RSA algorithm but little slower in speed. This document is meant to understand existing DNS security challenges and demonstrates best practices for secure deployment of DNS using digital signature for DNS data. Deploying and managing DNSSEC is at technique which requires proper planning, skillful DNS administrators and precise approach. Therefore to ensure DNSSEC proper deployment and its understanding, an effort is made in this paper to discuss security challenges of DNS and also demonstrated cryptographic framework with industry based best practices to deploy a secure DNS infrastructure with DNSSEC. It is suggested to implement DNSSEC based trusted DNS infrastructure, specifically for those domains whose parent domain have already signed and support DNSSEC. For DNS chain of trust as discussed TLD must be signed and support DNSSEC. Future work is required to enhance DNSSEC support in devices and strategy should adopt for deploying DNSSEC on TLDs domains which are still not signed with DNSSEC to form global DNS chain of trust, so that internet communication could be secure from forgeries at large scale.

VIII. REFERENCES

[1]. An Efficient Implementation Of The Digital Signature Algorithm P. Kitsos, N. Sklavos and O. Koufopavlou.

[2]. Carnegie Mellon Software Engineering Institute "Public Key Cryptography.

[3]. Robert D. Silverman, "An Analysis of Shamir's Factoring Device", RSA Laboratories, May 3, 1999.

[4]. R Gennaro. (2000), "RSA-Based Undeniable Signatures" Journal of Cryptology, Vol 13, No. 4, pp 397-416.

[5]. Knowledge Through Fun: DRAWBACKS OF USING DIGITAL SIGNATURE http://computerfun4u.blogspot.com/2009/02/drawbacks-of-usingdigital- signature.html?m=