International Journal For Technological Research In Engineering
Volume 3, Issue 10, June-2016 *ISSN (Online): 2347 - 4718*

COMPLEXITY COMPARISON OF ECDSA AND VARIANT ECDSA

Gourav Mitawa[1], Pardeep Kumar Sharma[2], Peeyush Mathur[3]
[1]PG Scholar, [2,3]Associate Professor, Sobhasaria Group of Institutions

Abstract: In DNS cache poisoning attack, an intruder substitutes a valid IP address cached in the DNS tabley with a rapscallion address. Requests addresses are redirected accordingly for the valid address and malwares (e.g., worm, spyware, browser hijacker etc.) may be downloaded from the rogue location to the user's computer. DNSSEC employs digital signatures and cryptographic keys to ensure that data to lookup is correct and that connections are to legal servers.DNS, Domain Name System is a protocol that resolves hostnames to IP Addresses over the Internet. DNS, being an open source, it is less secureand it has no means of determining whether domain name data comes from an authorised domain owner. So, these vulnerabilities lead to a number of attacks, such as, cache poisoning, cache spoofing etc. Hence, there is a need of securing DNS.Digital Signatures are a good way of authyenticating the domain owners. The digital signatures generated with public key algorithms have the advantage that anyone having the public key can verify them. Existing proposals include public key cryptographic algorithms (e.g., RSA, DSA etc.) for securing DNS. With the technology growing faster everyone accesses internet through mobile phones whether it is used to check E-Mails or visiting any secure sites, ECDSA involving ECC (Elliptic Curve Cryptography) concepts having less key sizes as compared to RSA can be implemented to provide security to DNS. DNS, Domain Name System is a protocol that resolves hostnames to IP Addresses over the Internet. DNS, being an open source, it is less secure 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, such as, cache poisoning, cache spoofing etc. Hence, there is a need of securing DNS.

KEYWORDS: DNS, RSA, ECDSA, DNSSEC, DSA and ECC.

I. INTRODUCTION

The Domain Name System is a protocol for locating domain names and mapping them to IP addresses. DNS is a hierarchical, distributed database, which provides mapping between easy to remember hostnames, such as www.RTU.ac.in, and IPv4 or IPv6 network addresses, for example, 117.211.115.134. Figure 1 shows a Domain Name System. In DNS tree , each node represents a DNS name. A DNS domain is a branch under the node. For example, uptu.ac.in is a DNS domain. When a hostname is translated into its numeric representation, this allows the network to trace a path from a user to a particular server. Correct and timely DNS translations are vital for networks such as the Internet and thus are an interesting target for attackers.

A. Working of DNS

Here we will be taking an example of getting the IP Address of "www.secs.ac.in", suppose it is 50.28.49.16.

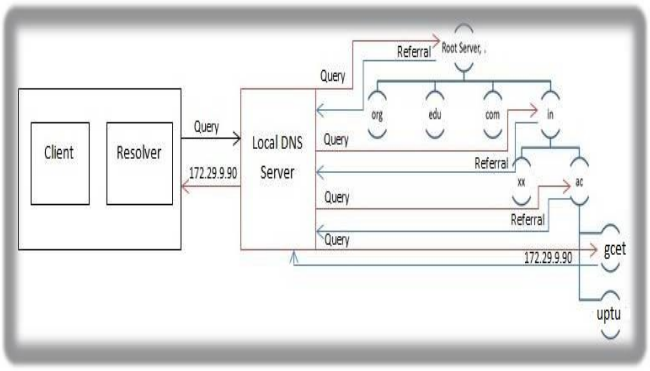


Figure 1.1 DNS Working

The left side of diagram shows the client side accessing internet to locate SEC, the right side shows the tree like representation (also called Domain Name Space) of getting to the site SEC.

Firstly, the Resolver checks in its cache, if it resides there then no need to proceed further.

B. DNS Security

As originally designed, DNS has no means of determining whether the domain name data comes from the authorized domain owner or it has been forged. This weakness in security leaves the system to be vulnerable to a number of attacks, like DNS cache poisoning, DNS spoofing etc. Due to weak authentication between DNS servers exchanging updates an attacker may predict a DNS message ID and manage to reply before the legitimate DNS server, thus inserting a malicious record into DNS database. One of the recent vulnerabilities of a DNS server structure is the ability of an attacker to insert false information into caching servers. The exploit forces a compromised DNS server to send a request to an attacker's DNS server, which will supply the wrong host to IP mapping.

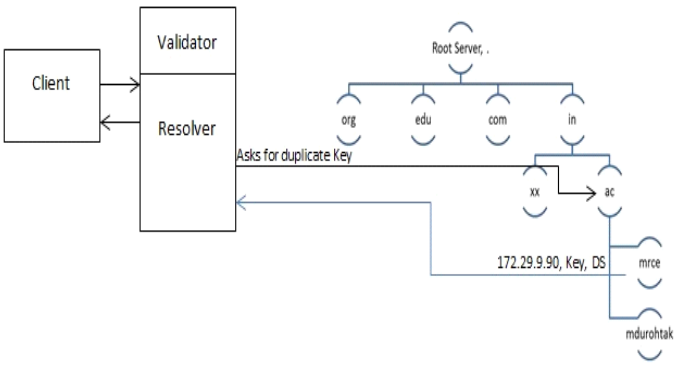


Figure 1.2 Idea of Security

C. Problem Statement

The ECDSA Applet is composed of one main class: the ECDSA class. This class implements the applet and performs all of the arithmetic computations and ECDSA functionality that the user requests when signing an IP Address on the applet or verifying a signature. The user can select from a list of curves with various key sizes to sign their address. Following is a summary of the functions and packages used to implement the ECDSA class. The ECDLP is the basis for the security and is based on the intractability of Scalar Multiplication products. Given points P and Q in the elliptic curve group, then find k such that, P.k = Q. k is a discrete logarithm of Q to the base p .this thing where the multiplicand can't be found even when the original and destination points are known is the basis of the security behind the ECDSA algorithm, and the principle is called a ECDLP or Trap Door Function. And if this Signature Verification is installed as software embedded in his/her browser, then he can verify the signature of the given IP Address. The user has nothing to do, he/she just has to sit back and wait for the IP Address to get authentic information. The backend where this functionality is embedded determines if the signature is valid given zone person's public key. The Applet shows this functionality as a module in it and on clicking "Verify Signature" button, a text field below the button shows the value of v to confirm that above shown r component is same as v and a message is displayed that the signature is valid or invalid. The generation of the public key in ECDSA involves computing the point, Q, where Q = dP. To crack the elliptic curve key, attacker would have to discover the secret key d. Given that the order of the curve E is a prime number n, then computing d given dP and P would take roughly 2n/2 operations. For example, if taken key length n is 192 bits (the smallest key m size recommended by NIST for curves defined over GF(p)), then attacker will be required to compute about 296 operations that takes around two and a half trillion years to find out the secret key.

II. SIGNATURE GENERATION ALGORITHM

Using A's private key, A generates the signature for message M using the given following steps:

Select a random number k to be used only once, that is, for every new signature generation of a message, a new k is selected, such that 1 < k < n-1

Generate (r, s) component of signature such that

- k.G = (x, y)
- r = x modulo n
- if r = 0 then repeat 2 again

Calculate hash of message (M) whose signature is to be generated, i.e., e = h(M)

$s = d(r*k - e)^{-1}$ modulo n //changed formula

A. Comparison RSA and ECDSA

Parameters	RSA	ECDSA
Key Size (same security)	1024 bit length Bigger	192 bit length
		Smaller
Signature Generation	Slow	Fast
Signature Verification	Fast	Slow
Encryption	Fast	Slow
Decryption	Slow	Fast
Key Exchange	Slow	Slow

Table 2.1 Comparison RSA and ECDSA

III. RESULTS

The purpose of using a Java applet is to provide a familiar and easily accessible medium for users to sign and verify messages using the elliptic curve digital signature algorithm. By using a Java applet, our implementation can be embedded into the software and made available for authoritative zones.

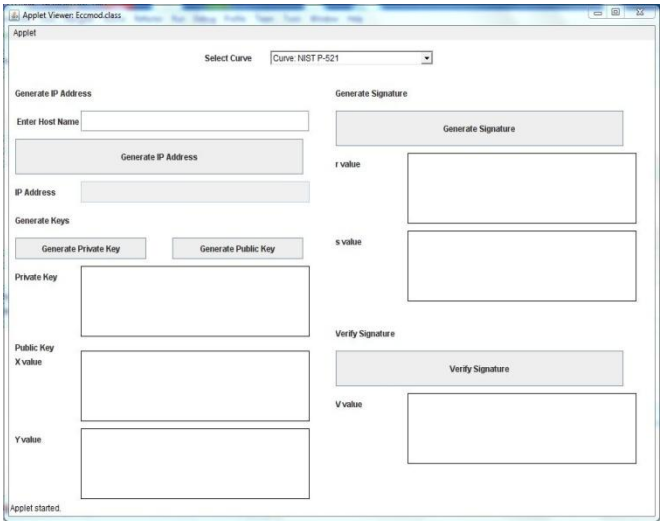


Figure 1.3 ECDSA Applet

Applet IP Address Generation:

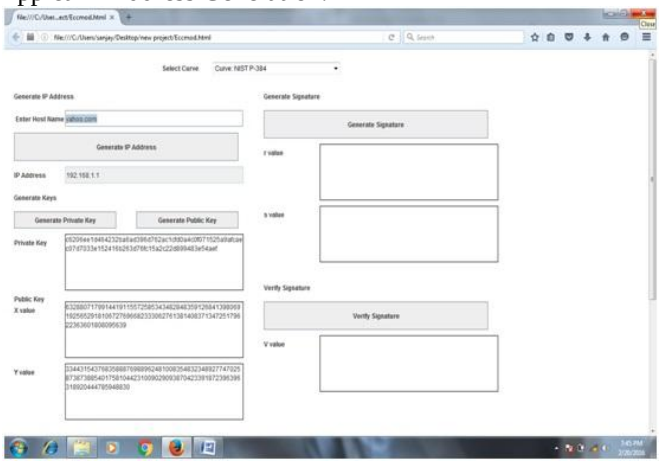


Figure 1.4 ECDSA Applet Generate Private Key

Applet Signature Generation:

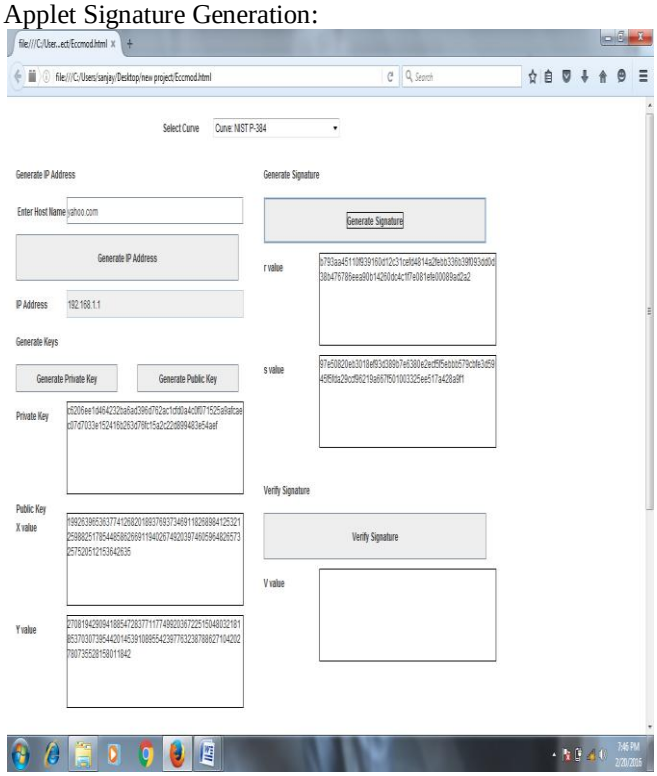
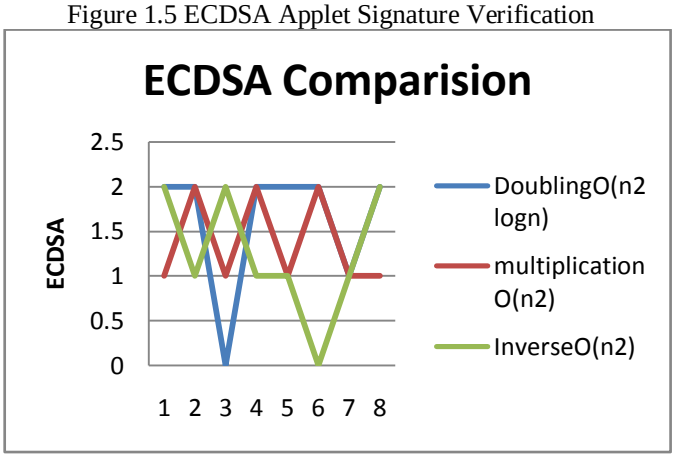


Figure 1.5 ECDSA Applet Signature Verification



IV. CONCLUSION

There are various security measures adopted in DNS using public key cryptography, which includes RSA and DSA. With the technology growing day by day, there is a need of same level of security with smaller key sizes. Now, everyone uses mobile to retrieve data from internet and mobile being small and portable device needs security with less power consumption. This can be done with the help of ECC by implementing ECDSA in DNS. ECC is a growing field of future. Blackberry has started to provide security using ECC.The implementation done in thesis work, shows a variant ECDSA algorithm that can be incorporated in software to build new DNS security provider software. The algorithm shows both signing and verifying operations wherein the signing process will take place at Zones and verifying process will take place at the client-side browser having valuator for the same.

REFERENCE

[1] Neetesh Saxena, Narendra S. Chaudhari, "Secure Encryption with Digital Signature Approach for Short Message Service", IEEE, 2012.
[2] Suranjith Ariyapperuma and Chris J. Mitchell, "Security vulnerabilities in DNS and DNSSEC", IEEE Computer Society
[3] Aqeel Khalique Kuldip Singh Sandeep Sood, "Implementation of Elliptic Curve Digital Signature Algorithm", International Journal of Computer Applications (0975 – 8887), Volume 2 – No.2, May 2010.
[4] Vivek Kapoor, Vivek Sonny Abraham, Ramesh Singh, "Elliptic Curve Cryptography", May 20-26, 2008. ACM Ubiquity, Volume 9, Issue 20.
[5] Nils Gura, Arun Patel, Arvinderpal Wander, Hans Eberle, Sheueling Chang Shantz, "Comparing Elliptic Curve Cryptography and RSA on 8-bit CPUs".
[6] Ramaswamy Chandramouli and Scott Rose, "Challenges in securing the domain name system", US National Institute of Standards and Technology, The IEEE Computer Society, 2006.
[7] Giuseppe Ateniese , Stefan Mangard , "A New Approach to DNS Security (DNSSEC)".
[8] D. Sravana Kumar, CH. Suneetha, A. Chandrasekhar, "Encryption of Data using Elliptic Curve over Finite Fields", International Journal of Distributed and Parallel Systems (IJDPS) Vol.3 (January 2012), No.1.
[9] Ghanmy Nabil, Khlif Naziha,, Fourati Lamia, Kamoun Lotfi, "Hardware implementation of Elliptic Curve Digital Signature Algorithm (ECDSA) on Koblitz Curves", 8th IEEE, IET International Symposium on Communication Systems, Networks and Digital Signal Processing.
[10] Kadjo Tanon Lambert, Oumtanaga Souleymane, Kone Tiemoman, Abba Brice, and Tety Pierre, "Deployment of DNSSEC: Problems and Outlines".

