Implementation Secure Authentication Using Elliptic Curve Cryptography
N.Thangarasu
thangamaru14@gmail.com

Abstract- Elliptic curve cryptography is the most efficient public key encryption scheme based on the elliptic curve concepts that can be used to create faster, smaller, and efficient cryptographic keys. As a use of network increase for critical transaction, so huge damages are caused by intrusion attacks hence there is the need of computer network security. To protect network against various active and passive attack, various technique have been suggested. Mobile devices have many differences in their capabilities, computational powers and security requirements. The security of mobile communication has stopped the list of concerns for mobile phone users. Confidentiality, Authentication, Integrity and Non-repudiation are required security services for mobile communication.

Keywords: - critical transaction, Intrusion attacks, Autonomous Security, Mobile communication security, Public key cryptography, Authentication, Integrity and non-repudiation.

I. INTRODUCTION

Rapid development on electronic technology secure communication in particular is in demand for any kind of communication network. The main components of secure communications software stack includes key exchange and signature which is required for public key algorithms like RSA, DSA and elliptic curve cryptography [1][2]. Elliptic curve system is applied to cryptography were first proposed in 1985 independently by Neal Koblitz and Victor Miller. The discrete logarithm problem on public curve groups is believed to be more difficult than the corresponding problem in the underlying finite field [3][4][5]. Public key cryptography is effective security solution to provide secure mobile communication [6]. ECC is the most efficient public key encryption scheme based on elliptic curve concepts that can be used to create faster, smaller, and efficient cryptographic keys. ECC can be used with public key encryption methods, such as RSA, and Diffie-Hellman key exchange communication privacy through encryption, authentication of sender and digital signature to ensure message integrity[7]. ECC can help to establish equivalent security with lower computing power and battery resource usage. Public key cryptography algorithms provide the way to achieve security requirements viz; confidentiality and authentication [8]. Network attack detection is the very challenging task for the network operator in today’s Internet. It is begin challenging task because network attack are moving targets, they are not steady. Attacker may launch every time new attack. The need of detection system that will be able to detect various attacks of different range and with variety of characteristic [9]. Commercial detection systems there are two different approaches namely Signature based detection and anomaly detection for detection of attack. Signature based detection can be used for pattern of unauthorized behaviour. Anomaly detection can be used for abnormal pattern behaviour.

II. CRYPTOGRAPHIC TERMINOLOGY

A security protocol formally specifies a set of steps to be followed by communicating parties, so that the mutually desired security objectives are satisfied. The four main security objectives include:

- **Confidentiality**: This means that the secrecy of the data being exchanged by the communicating parties is maintained, i.e., no one other than the legitimate parties should know the content of the data being exchanged.
- **Authentication**: It should be possible for the receiver to ensure that the sender of the message is who he claims to be, and the message was sent by him.
- **Integrity**: It provides a means for the receiver of a message to verify that the message was not altered in transit. It checks originality of message.
- **Non-repudiation**: The sender of a message should not be able to falsely deny later that he sent the message, and this fact should be verifiable independently by an independent third-party without knowing too much about the content of the disputed messages.

III.APPLICATIONS OF PUBLIC KEY CRYPTOSYSTEM

Some public key algorithms are ECC, RSA, Diffie-Hellman key exchange and DSA. In the later section we mainly focus on Elliptic Curve Cryptosystem (ECC). Table1

<table>
<thead>
<tr>
<th>Algorithm</th>
<th>Encryption/decryption</th>
<th>Digital signature</th>
<th>Key exchange</th>
</tr>
</thead>
<tbody>
<tr>
<td>RSA</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Elliptic Curve</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Diffie-Hellman</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>DSS</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

Table.1 applications of public key cryptosystem
IV. ELLIPTIC CURVE CRYPTOGRAPHY

The principal attraction of Elliptic Curve Cryptography (ECC) compared to RSA is that it offers equal security for a far smaller key size, thereby reducing processing overhead. The advantage of ECC over other public key cryptography techniques such as RSA is that the best known algorithm for solving ECDLP the underlying hard mathematical problem in ECC takes the fully exponential time and so far there is a lack of sub exponential attack on ECC. ECC is based on the Discrete Logarithmic problem over the points on an elliptic curve [8][10][11].

Elliptic curve is the set of Weierstrass equation of the form

\[ Y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \]  
\[ Y^2 = x^3 + ax + b \]  
\[ Y^2 = x^3 + ax^2 + b \]  
\[ Y^2 = x^3 + ax + b \]

Cryptography purposes we always use a finite field \( a_1, a_2, a_3, a_4, a_6 \) are real numbers belong to \( R \), \( x \) and \( y \) take values in the real numbers. If \( L \) is an extension field of real numbers, then the set of \( L \)-rational points on the Elliptic curve is called Weierstrass equation. The following algorithm gives the points on the curve Eq2 (a,b) [12].

Algorithm elliptic-points \((p,a,b)\)

\[
\begin{align*}
X &= 0 \\
\text{While}(x < p) \\
W &= (x^3 + ax + b) \mod p \\
\text{If} \ (w \text{ is perfect square in } Zp) \\
\text{Output} \ ((x\sqrt{w}),(x, - \sqrt{w})) \\
X &= x + 1 \\
\end{align*}
\]

The number of points on an elliptic curve over a finite field must satisfy Hasse’s theorem. The order of the curve \( N \) will satisfy the following equation [8][10][12].

\[ P + 1 - 2\sqrt{p} \leq N \leq P + 1 + 2\sqrt{p} \]

\[ \text{Point Doubling} \]

\[ \text{Point Additions} \]

Point additions (PA) and point doublings (PD) can be implemented using coordinate system [13] like affine coordinate system, standard projective, Standard projective and affine, Jacobian projective and affine, lopez-Dahab. The most popular coordinate representation is affine repetition which is based on two coordinate \((x,y)\) and other representation such as projective Jacobian, lopez-dahab uses three coordinates. Transforming affine coordinates into one of the other representation is almost simple but not vice versa, since transformation requires costlier field inversion[3][7]. The addition of two points on an elliptic curve. Elliptic curves have the interesting property that adding two points on the elliptic curve results a third point on the curve. Therefore, adding two points, \( P_1 \) and \( P_2 \), gets us point \( P_3 \), also on the curve. Small changes in \( P_1 \) or \( P_2 \) can cause a large change in the position of \( P_3 \). Point addition is the addition of two points \( J \) and \( K \) on an elliptic curve to obtain another point \( L \) on the same elliptic curve and point doubling is the addition of a point \( J \) on the elliptic curve to itself to obtain another point \( L \).

V. SECURITY OF ELLIPTIC CURVE CRYPTOGRAPHY

Security is the most attractive feature of elliptic curve cryptography. Elliptic curve cryptosystems also are more computationally efficient than the first generation public key system like RSA, DSA and Diffie-Hellman key exchange algorithm. Table 1 gives approximate equivalent key size for ECC and RSA algorithm.
From table 1 it is clear to see that ECC affords the same security as RSA while using significantly smaller key sizes. In Table 1, at all levels of security including 512 bits, ECC has smaller public key sizes than both RSA and DSA/DH. Because of its smaller key size, ECC outperforms both RSA and DSA/DH for most routine operations while offering comparable levels of security. The reason is that ECC provides greater efficiency in terms of computational overheads, key sizes and bandwidth. In implementations, these saving mean higher speeds, lower power consumption. For efficient cryptosystem implementation ANSI (American National Standard Institute) and NIST (National Institute of Standard and Technology) are producing standards and technology [3][8].

<table>
<thead>
<tr>
<th>Time to break in MIPS years</th>
<th>RSA/DSA key exchange</th>
<th>ECC Key size</th>
<th>RSA/ECC key size ratio</th>
</tr>
</thead>
<tbody>
<tr>
<td>$10^7$</td>
<td>512</td>
<td>106</td>
<td>5:1</td>
</tr>
<tr>
<td>$10^9$</td>
<td>768</td>
<td>132</td>
<td>6:1</td>
</tr>
<tr>
<td>$10^{11}$</td>
<td>1024</td>
<td>163</td>
<td>7:1</td>
</tr>
<tr>
<td>$10^{20}$</td>
<td>2043</td>
<td>210</td>
<td>10:1</td>
</tr>
<tr>
<td>$10^{28}$</td>
<td>21000</td>
<td>600</td>
<td>35:1</td>
</tr>
</tbody>
</table>

Table 2. Security of Elliptic Curve Cryptography

VI. NETWORK DETECTION METHOD

6.1. Anomaly Detection: Anomaly detection is used in the data mining based intrusion detection system tries to define what is normal and then detect how analyzed data is different from model [14]. But meanwhile if some intrusion arises, it will not be considered as normal. It detects them initially. It is also possible that training data will contain traces of intrusion, so in such case future instance of the attack may not be detected rather; they will be treated as normal.

6.2. Misuse Detection: The set of labelled data is used to train the machine learning algorithm and the detection model is built. This detection model will be similar to the signature describe earlier. But this is also similarly vulnerable to new type of attack as the signature based method.

VII. UNSUPERVISED NETWORK ATTACK DETECTION

Aiming at discovery knowledge independent system, new proposed algorithm is unsupervised network attack detection algorithm. Initially traffic is captured and packet are analysed by aggregating in multi resolution flow. On the top of these flow, different time series is built. And anomalous change is defined by change-detection algorithm based on time-series analysis.

7.1. Determining degree of abnormality: There is the use of robust clustering algorithm like sub-space clustering (SSC), Density-based clustering, and Evidence Accumulation Clustering (EAC) as combination of these approaches for providing traffic structure. These traffic structures are used as the evidence for determining by how much degree the traffic is not normal. Thus the output of second stage is outlying flow.

7.2. Declaring anomalies: Using a simple threshold detection approach, outlying flow which is top ranked is flagged as anomalies.

VIII. UNSUPERVISED ATTACK DETECTION THROUGH CLUSTERING

IP flows in the flagged time slot are used as the input for unsupervised attack detection. At this step unsupervised network attack detection algorithm ranks the degree of abnormality of every flow by using clustering and outliers analysis techniques. Two different resolutions, using either IP source or IP destination aggregation key IP flows are analysed. There are two different anomalies on the basis of which traffic anomalies can be classified, 1-to N anomalies and N-to-1 anomalies.

IX. PERFORMANCE PARAMETERS FOR ELLIPTIC CURVE CRYPTOGRAPHY IMPLEMENTATION

Although RSA, El-GAMAL and Diffie-Hellman are secure asymmetric key cryptosystem, their security comes with a price, their large keys. So researchers have looked for providing substitute that provides the same level of security with smaller keys. For Elliptic Curve Cryptography implementation following consideration should meet [1][15][16][17]:

- Suitability of methods available for optimizing finite field arithmetic like addition, multiplication, squaring, and inversion.
- Suitability of methods available for optimizing elliptic curve arithmetic like point addition, point doubling and scalar multiplication.

- Application platform like software, hardware, or firmware.
- Constraints of a particular computing environment e.g., processor speed, storage, code size, gate count, power consumption.
- Constraints of a particular communications environment e.g., bandwidth, response time.
- Suitability of methods used for optimizing anomaly detection, misuse detection, unsupervised network attack detection, unsupervised attack detection through clustering.


Dr. R. S. Shanmugalakshmi and M. Prabu “Prospective Utilization of Elliptic Curve Cryptography for security Enhancement” International Journal of Application or Innovation in Engineering & Management (IJAEM), Volume 2, Issue 1 January 2013


Pradeep Malik “Elliptic Curve Cryptography for security Inwireless Networks” Statistics 2011 Canada: 5th Canadian Conference in Applied Statistical Techniques, July 1-4, 2011, Concordia University, Montreal, Quebec, Canada.

LIU Shuanggen, LI Ping, HU Yupu “improvement Schemes for Scalar Multiplication Algorithm in Elliptic Curve Cryptography” ISSN: 1000-3428, 2006-17-009.


Xue Sun, Mingping Xia “An improved proxy signature based on elliptic curve cryptography” DOI:10.1109/ICCCS.2009.36.