Chapter 12

Countering RSA Vulnerabilities and Its Replacement by ECC: Elliptic Curve Cryptographic Scheme for Key Generation

Behnam Rahnama
ScaleDB Inc., USA

Arif Sari
Girne American University, Cyprus

Marwan Yassin Ghafour
Sulaimani Polytechnic University, Iraq

ABSTRACT

Security is utilized to keep the information safe. Online resources, e-commerce, internet banking and a lot of similar services are protected by use of well-known protocols such as Secure Socket Layer (SSL). This protocol makes use of the RSA key exchange protocol for authentication. New innovations and boosts in the computational power of supercomputers today makes it quite easier than before to break through RSA and consequently decrypt the payload transferred over SSL. In this research demonstrates the use of SSL; how to utilize it in the best shape? We also discuss reasons of why we need to improve its strength. The proposed solution is to replace the RSA key exchange mechanism utilized in SSL with Elliptic Curve Cryptography (ECC).

INTRODUCTION

In many life situations, we have private information that necessitates protection from illegal access. In order to give protection to our sensitive information and avoid any unauthorized access to it, the digital world offers us techniques using cryptography.

The aim of cryptography is to give protection to information while it is being transmitted between two parties, and avoiding access to any third illegitimate party who attempts to obtain a part of it through

DOI: 10.4018/978-1-4666-8761-5.ch012
Countering RSA Vulnerabilities and Its Replacement by ECC

prohibited means. Our aim is to improve current methods of combating such hackers aiming to obtain unauthorized access.

In the digital world, many applications and situations benefit from cryptography. Just a small selection includes but not limited to ATMs, SSL web based applications within browsers, authentication and authorization acceptance and server-client applications, military services, electronic commerce and satellite communication (Stallings, 2005; Cole, et al., 2008).

Problem Definition

The Secure Sockets Layer (SSL) protocol works alongside operations to perform the highly important task of transmitting our confidential data securely between authorized parties; the RSA algorithm is one of three components it uses to complete this task. Due to digital development and our growing use of the computing world to distribute our most sensitive information, such as banking details and even national security details, these days it has become highly important to provide a safeguard to protect these transmissions from attackers. A constant attempt to invade privacy with new techniques exists today, and therefore a primary aspiration should be to find a suitable algorithm to prevent attacks while neither slowing down a device not requiring extra resources.

Working Principles of SSL

SSL is a protocol, which was developed in 1994 by the Netscape Company, to establish a secure data transaction over a secure link between servers and their clients. Normally it is established on a trusted connection like TCP.

This protocol provides authentication by exchanging a key set of a public key algorithm like RSA, and a symmetric key algorithm like DES or RC4 for the encryption of transmitted messages (confidentiality), and one of MAC algorithms for preventing editing of a message by an attacker in the middle (integrity).

The function of this protocol is to encrypt sensitive, restricted or personal information, of which banking, military or governmental data constitute principal examples, where illegal interception of data by a third party could cause critical adverse. The protection of SSL being present is demonstrated on webpages by the letters https at the beginning of the URL with a small lock icon beside it declaring that any communication passing between web server and browser is encrypted, and therefore regarded as being secure.

The SSL can be used on any website that has a requirement to send and receive highly sensitive data which could incorporate credit card numbers or other such private information. Transmission of such data without use of SSL, can disclose the information to unauthorized parties and cause enormous damage. The procedure of an SSL connection would ensue in the following manner. At first instance, a client makes a connection to an SSL website, which is indicated by the letters https at the beginning of the address. The website then sends the client its public key; the client’s browser confirms if key is valid and trustworthy by checking the site’s digital certificate. Various checks are done to pursue this action. For example, the authentication of the issuer and the expiry date is checked accordingly. Client’s browser verifies and confirms the server’s public key. The server uses a unique hash for the encryption, which is encrypted using the client’s public key and it is returned to the client for future use. The client’s browser decrypts the message, and it enables the client to read sent messages. Finally, server and client can conduct an exchange of information with the assurance that the communication is totally secure.