Guillou Quisquater Protocol

Prepared by-
Soumyadeep Basu - IIT2018001
Kumar Utkarsh - IIT2018007
Rohit Haolader - IIT2018008
Raushan Raj - IIT2018031
Suryasen Singh - IIT2018069

Abstract

A Zero knowledge Authentication is a protocol between two parties called the Claimant and the Verifier. In the Zero Knowledge Authentication, anything which may increase the danger of confidentiality of the secret is not revealed by one party, which is called the claimant. The claimant simply has to prove the other part called the verifier that it knows a secret, without telling it.

Introduction

In this protocol, the prover proves to the verifier that they know the v^{th} root (1/B) modulo n of a given number J ∈ Z/nZ. The prover has a public key which is (J,v,n) and B is the private key. The basic working of this protocol is as follows:

- Prover chooses a random number and does a computation whose result is then sent to the verifier.
- The verifier chooses a random number based on the number sent by prover and sends it back.
- The prover then does a computation with this received value and sends back the result for verification.

Method

- System Parameters
  - Private: p, q, s=v-1 mod (n)
  - n=pq, v >2

- User Parameters
  - The secret of A with JA=f(I_A) is J_A-s mod n

- Protocol Messages (Repeat t times)
  - A sends to B(Commit): I_A, $x=r^v$ mod n for a random r
  - B sends to A(Challenge): a random e with 1=<e=<v
  - A sends to B(Response): $y=r\ s_A^e$ mod n

- Verify
  - B computes $z=J_A^e y^v$ mod n
  - Accept A's proof of identity if z = x and z 0

Example

Method

With the GQ method, Peggy (the prover) has a proving public key of (N,e,X) and a proving secret key of (N,x). N is a prime number for the modulus operation. In this case x is the secret, and where:

$X=x^e(\mathrm{mod}N)$
On the registration of the secret, Peggy generates a random value (y), and then computes Y:

$Y\leftarrow y^e(\mathrm{mod}N)$
This value is sent to Victor (who is the verifier). Victor then generates a random value (c) and sends this to Peggy. This is a challenge to Peggy to produce the correct result. Peggy then computes:

$z\leftarrow yx^c(\mathrm{mod}N)$
She then sends this to Victor in order to prove that she knows x. Victor then computes two values:

$val1=YX^c(\mathrm{mod}N)$
$val2=X^e(\mathrm{mod}N)$
If the values are the same ($val1\equiv val2$), Peggy has proven that she knows x.

This works because:
$YX^c=y^e(x^e)^c=y^ex^{ec}$
$z^e=(yx^c)^e=y^ex^{ec}$

Security Analysis

Consider we have an attacker and we have two users Alice and Bob:

- Attack 1: If attacker knows Alice's public key, he intercepts the values (i.e d and t) and computes the scalar T using the equation, but it won't work, because he must send the value of T at the beginning of the procedure.

- Attack 2 :Since he must need to solve the equation with two unknowns B and r. So even If the attacker intercepts the value of t he won't be able to find Alice's secret key.

- Attack 3 : If the attacker intercepts the value of T and t, he will still be blocked at the challenge number of d which is changeable at each identification.

Conclusions

- We have described the Guillou-Quisquater Protocol which is based on the concept of **zero-knowledge proof** and analyzed it's security along with the algorithm it uses for this security.
- Although it is quite strong, but still it has certain limitations due to **RSA's assumed one-wayness.**