Internet-Draft R.Nagpal
draft-nagpal-biometric-digital-signature-00.txt S.Nagpal
Intended Category: Informational Asian School of Cyber Laws
Expires: October 2002 May 2002

Biometric based Digital Signature scheme

Status of this Memo

1. Abstract

Digital Signatures are fast emerging as a viable information security solution, satiating the objectives of data integrity, entity authentication, privacy, non-repudiation and certification.

The technique, as it stands today, faces the problem of the maintenance of the secrecy of the private key. This document provides a conceptual framework for the establishment of a biometric-based key generation scheme. In this scheme, the private key is generated each time a document or record requires to be signed. Such generation is based upon a combination of biometric traits.

The key words "MUST", "REQUIRED", "SHOULD", "RECOMMENDED", and "MAY" in this document (in uppercase, as shown) are to be interpreted as described in RFC 2119.

2. Pre-requisite for reading this document

A certain basic knowledge of cryptography and Digital signatures would be helpful in understanding this document.

3. Overview of present system

In a digital signature scheme, a person first generates two

mathematically related keys (simply put, a key is a number), a private key and a corresponding public key. Calculating the private key from the public key is considered computationally infeasible. The public key is revealed to the world at large whereas the private key is kept secret.

Digital signatures are created using the private key while they are verified using the coressponding public key.

A compromise of the private key can cause security breaches of very large magnitude. Maintaining the secrecy of the private key poses a problem within the present system.

4. Biometrics

Biometrics is the use of some physiological or behavioural characteristics for authentication and identification. This technique of authentication is based upon the fact that certain characteristics are never the same in any two people.

Biometric recognition systems operate in two modes - one is the identification where the system identifies a person by searching a large database for a match and the other the authentication mode where the systems verifies a person’s claimed identity by checking against a previously entered pattern.

The techniques included in this method of identification are retina scanning, iris scanning, fingerprint verification, voice verification, facial analysis etc. Biometric based authentication schemes are utilized in sectors like Public services, Law Enforcement and Banking.

5. Current method of key generation

One of the most popular asymmetric encryption schemes is the RSA algorithm, which goes as under:

Take two large prime numbers say ’p’ and ’q’.

Calculate N = pq

Calculate A = (p -1) (q -1)

Find a number E such that 1 < E < A and that E and A are coprime

Find a D such that 1 < D < A and ED is congruent to 1 mod A.

Now, the private key of a person is (N, D) and the public key is (N, E).

Currently the key generation is handled by software applications

that randomly choose the numbers ’p’, ’q’ and ’E’.
Once generated, the private key ’D’ is supposed to be kept securely. For signing any document this private key needs to be used and hence it needs to be securely stored.

6. Proposed method of key generation

The authors propose a biometric-based key generation scheme, which would function something as follows:

a. Firstly a person would visit his bank (or some other Government authorised agency). There her / his retina, iris and fingerprint (Note: any other combination of biometric traits can be used) would be scanned.

b. The result of the retina scanning would be a large number (a suitable algorithm that always gives a fixed number for a fixed retina pattern has still to be developed, though!). If this number is a prime number it will be taken as 'p' as per the formula in section 4 above. If this number is not a prime number, then it will be incremented by one till a prime number is obtained and then this prime number now obtained will be treated as 'p'.

c. The result of the iris scanning would be another large number (a suitable algorithm that always gives a fixed number for a fixed iris pattern has still to be developed, though!). If this number is a prime number it will be taken as 'q' as per the formula in section 4 above. If the generated number is not a prime number, then it will be incremented by one till a prime number is arrived at and then this prime number now obtained will be treated as 'q'.

d. According to section 4 above the next step would be to get 'N' which is the product of 'p' and 'q'.

e. Fingerprinting the person shall provide the third large number required, 'E'(a suitable algorithm that always gives a fixed number for a fixed retina pattern has still to be developed, though!). E has to be greater than 1 and less than A and E and A are co-prime. Thus in the next step the system shall attempt to satisfy both these conditions by reducing (or incrementing) the number generated by 1 time till the conditions are met.

f. Having obtained the relevant numbers, the private key and the public key can be generated.

7. Moral of the Story

The private key of the person would be generated every time that the person wishes to sign (or for that matter decrypt) a record. His public key, on the other hand will always be taken from the records of the bank (or other Government appointed agency) where

the key pair was first generated.
An elaborate key revocation protocol would have to be worked out based upon current practices with relevant modifications.
The private key should be allowed to sign as long as the iris, retina and fingerprint of the person are in adequate physical proximity to the system. Once that proximity is lost, the private key should be permanently erased by the system.

8. Applications

This method of key generation would ensure the trust of the public in cryptography and digital signatures to a much larger extent. It would be possible to utilize this method in many applications requiring authentication or identification.

a. Banking transactions

When a person goes to a bank to open an account he will be asked to fill out an electronic form. Then he will place his head in front of a console where his retina and then iris shall be scanned. On the same console shall be provided the facility for fingerprinting. While the above processes are taking place the scanning computer may be disconnected from the network thus transforming it into a stand-alone machine. Once this is done and the keys generated, he will sign the electronic form using the private key. The private key will then self-destruct, leaving no trace of it anywhere even on the generating computer.

The public key shall be backed up with the bank. One copy of it shall be given to the customer and one copy shall be provided to the Certifying Authority working in association with the bank. The Certifying Authority shall certify the public key by issuing the relevant digital signature certificate.

The ATM card provided to the customer will contain his public key apart from other details. Now every time that the person wants to withdraw money, he will go to the ATM centre, wherein he will fill in an electronic form stating that he wishes to withdraw a particular amount. When he presses submit, a console will open up allowing him to scan his retina and iris and record his fingerprint. He will first unplug the machine making it stand-alone. The private key generated in this way will be used to sign the request. Once the signature is made the key shall be destroyed. The money will be withdrawn on this basis.

The introduction of such a process in banking shall rid the customer of another very widely prevalent problem - that of wrongful use of someone else’s ATM card. This way even if a person does steal or get access to a card, he will not be able to authenticate himself for signing the final request.

b. Electronic Contracts

A similar process may be used to authenticate electronic contracts. The contracting parties shall sign the contract after having created their private keys on the spot. Since all the criteria for key generation will be followed this system shall allow for signature and verification of all contracting parties to an electronic contract.

c. Credit card payments

This procedure may further be used for credit card based

transactions. The credit card shall store the public key of the person. The private key will have to be generated at the moment of signing and will be destroyed once its requirement is over.

9. Security Considerations

The security of the biometric based key generation system is based upon the integrity of the systems used by the agencies involved i.e the Certifying Authorities, Banks etc.

10. Acknowledgments

The authors gratefully acknowledge the contributions of Debasis Nayak and Abhinav Bhatt, whose review and comments significantly clarified and improved the utility of this document.

11. Authors' Addresses

Rohas Nagpal
Asian School of Cyber Laws
6, Rajas, Pashan Road,
Opp Abhimanshri,
Pune 411008, INDIA

Email: rn@asianlaws.org

Shuchi Nagpal
Asian School of Cyber Laws
6, Rajas, Pashan Road,

Opp Abhimanshri,
Pune 411008, INDIA

Email: sn@asianlaws.org