

Mutual Authentication-robust user Authentication for Online Services

¹V. Uma Maheswari, ²S. Anitha Reddy

¹Dept. of CSE, Vardhaman College of Engineering, Shamshabad, Hyderabad, AP, India

²Dept. of CSE, Krishna Murthy Institute of Technology and Engineering, Edulabad, Ghakesar, AP, India

Abstract

The purpose of this paper is to present an improvement of the Needham-Schroder public key protocol. This new protocol will use partial quotients issue from the continued fraction expansion of some irrational numbers to secure the authentication between two principals. We introduce a new approach in the use of pseudo-random numbers, because besides using these numbers to provide uniqueness and timeliness guarantees, we use them to ensure that nobody can guess the identity of the sender. We also keep this new protocol secure against the Lowe attack, without taking the solution suggested by Lowe. This protocol remains fast although we compute some partial quotients during the authentication process.

Keywords

Authentication, Continued Fraction, Cryptography

I. Introduction

The alarming increase in victims of impersonation and the need to secure emerging tools as cloud computing imply the necessity to improve existing authentication protocols.

As defined by Menezes et al [11], entity authentication is the process whereby one party is assured (through acquisition of corroborative evidence) of the identity of a second party involved in a protocol, and that the second has actually participated (i.e., is active at, or immediately prior to, the time the evidence is acquired).

The mutual authentication, also called two-way authentication, is a process in which both entities authenticate each other. In this paper, it is the definition that we will adopt.

There exists several authentication protocols including: Kerberos [16], Needham-Schroeder [12], Wide Mouthed Frog [3], Woo-Lam [18]. Some protocols are based on others such as Kerberos which is based on Needham-Schroeder.

The Needham-Schroeder protocol has two variants, the first one is based on symmetric cryptography and the second one is based on public key cryptography. In this paper, we will focus on the version based on the public key cryptography.

This protocol has been widely studied [5] since 1978 but the greatest improvement was made in 1995, when Lowe [10] proved that this protocol was sensitive to the impersonate attack. The improved version Needham-Schroeder-Lowe seems to be strong until now and currently most studies, on this protocol are oriented on the security proof.

The improvement of the Needham-Schroeder protocol introduced in this paper will be partly based on the fact that the continued fraction expansion of an irrational number is unique. Also, it will be based on the difficulty of retrieving an irrational number from the sole knowledge of a part of its continued fraction expansion.

Continued Fractions: An expression of the form

$$\alpha = a_0 + \frac{b_0}{a_1 + \frac{b_1}{a_2 + \frac{b_2}{\ddots}}}$$

is called a generalized continued fraction. Typically, the numbers may be real or complex and the expansion may be finite or infinite.

is called a generalized continued fraction. Typically, the numbers may be real or complex and the expansion may be finite or infinite.

We will avoid the use of the continued fraction expansions involving $B_i=1$ for most i 's. However, in order to simplify our explanation we will use in some cases the classical continued fraction expansion, namely $B_i=1$ for any i :

In this paper we denote by the combined sets of algebraic irrationals of degree greater than 2 and transcendental numbers. Our algorithm, will use the irrational numbers which are in , but we will avoid the use of transcendental numbers having a predictable continued fraction expansion (some examples of irrational numbers with a given predictable continued fraction expansion are presented in [1-8].

To calculate the classical continued fraction expansion of a number, write down the integer part of . Subtract this integer part from . If the difference is equal to 0, stop; otherwise find the reciprocal of the difference and repeat. The procedure will halt if and only if is rational.

We can enumerate some continued fractions properties:

1. The continued fraction expansion of a number is finite if and only if the number is rational.
2. The continued fraction expansion of an irrational number is unique.
3. Any positive quadratic irrational number has a continued fraction which is periodic from some point onward, namely a sequence of integers repeat (Lagrange Theorem).
4. The knowledge of the continued fraction expansions of and cannot determine simply those of or.

Continued fractions were widely studied by Olds [13] and Perron [14], but cryptographic views are not explored by number theory specialists except in some areas like RSA cryptanalysis. In addition to the RSA cryptosystem, continued fractions are used to build a stream cipher [6] or to set up a e-cash scheme [7].

This paper is organized as follows: In Section 2 we will propose and demonstrate some results concerning continued fractions; in Section 3, we will introduce the Needham-Schroeder protocol. In Section 4 we present our new protocol, and before the conclusion, we will compare to the two algorithms.

A. Preliminaries

The Result 1 and the Result 2 have already been presented in [6-7].

The Result 2 will exhibit an example of irrational number which we can use in our protocol.

The Result 1 shows that the intruder will not succeed if he tries to impersonate the principal in the last attack of Section 4.5.

II. The Needham-Schroeder Protocol

2.1 The Needham-Schroeder Protocol

As defined in [12], the public key protocol consists on the following

seven steps:

Step 1: $A \rightarrow AS$

The exchange opens with A consulting the authentication server to find B's public Key.

Step 2: AS responds with: $E(\{PK_b, B\}:SK_{AS})$.

Where SK_{AS} is the authentication server's secret key, PK_b is B's public key and B is B's identity.

Step 3: A sends to B the following $E(\{Na, A\}:PK_b)$.

This step is for the communication with B to be initiated. This message, which can only be understood by B indicates that someone purporting to be A wishes to establish communication with B. B decrypts the message with his private key and then finds the nonce chosen by A.

Steps 4 & 5: B finds A's public key (PK_A) with steps similar to 1 & 2.

Step 6: At this point B return the nonce, along with a new nonce, to A, encrypted with A's public key ($E(\{Na, Nb\}:PK_A)$)

Step 7: At the end, A returns the nonce to B, encrypted with B's public key.

III. Our Contribution

The improvement proposed here is based on the work of Lowe, since we have solved the previous attack without his solution described above.

As for the Needham-Schroeder algorithm we suppose that communications are carried on an insecure channel.

We denote by $FC(X, Y)$ the first ten partial quotients issue from the continued fraction expansion of the irrational number X and Y where is a vector of ten B_i 's (we recall that the B_i 's are used during the computation of the generalized continued fraction).

We denote by $FC'(X, Y)$ the nine partial quotients following the first one in the continued fraction expansion of X (the first partial quotient is ignored in the authentication protocol).

We denote by Y_a, Y_b or Y_i the vectors used in the computation of the generalized continued fraction as described in the introductory paragraph.

Remark:

1. We suppose that we are in the case of an identity-based cryptosystem in which KC issues a private key to a registering user and uses the user's identity as his public key.
2. The status of the key (revoked or not) will depend on the security given by identity-based cryptosystem.
3. The first partial quotient is ignored because it does not change regardless the chosen.

The forced delay attack

This attack does not have a real influence on our algorithm because there is no timestamp. Hence, the behaviour of the principals will be the same even if someone intercepts the message and relays it later.

Remark

We recommend the use of the generalized continued fraction instead of the classical continued fraction; because the classical continued fraction produces a several partial quotients with only one digit [9], while the partial quotients obtained from some generalized continued fraction seems to be indistinguishable by all polynomial-time statistical tests from the uniform distribution of integers [6].

IV. Comparison with Needham-Schroeder-Lowe

A. Comparison

The Needham-Schroeder-Lowe protocol used nonces where we use continued fraction expansions and nonces, so it is clear that our algorithm is more expensive in terms of computation time, however we strongly believe that our scheme is more secure than the algorithm of Needham-Schroeder-Lowe. Our protocol increases the level of security with the introduction of continued fraction and if we consider that the calculations are done in two phases, the preparation phase can reduce the time needed for the authentication itself.

We have greatly simplified the Needham-Schroeder-Lowe protocol, because in addition to the number of steps which we have reduced, we also removed the identities of the principals in messages. It is a great progress to remove the identity of the principal in the protocol because if the secret key of the principal A fell into the wrong hands, the attacker could use this key to impersonate A, while in the new protocol, the intruder will not be able to identify the other principal.

V. Identity

The problem of removing identities should be more studied in authentication protocols because for security reasons, it is not conceivable to let the identity of the principal anywhere (web merchant, webmail, website, forum ...).

Although, it will be difficult to remove completely the identity, we are sure that we can reduce it to a minimum.

Several solutions such as the anonymous credential systems or group signatures have been proposed in the past, unfortunately, these systems have not yet been deployed on a large scale [19].

We add to these existing solutions, two new proposals.

The first one is the complete removal of the explicit identity if it can be guessed.

We note here that identity will always be present in the authentication protocol but implicitly.

The identity may be inferred, for example, when a company has only one client at King Street, it would be easy to omit the identity of that client.

Or if a company has five customers on King Street, and among them one who connects every day at 7 am, we can also omit the identity of this customer on the authentication protocol.

Finally, we can try to find from artificial intelligence tools, some solutions which will allow us to guess who is the entity who wants to connect instead of mentioning explicitly its identity.

The second solution which we propose is the separation between the explicit identity and authentication protocol itself.

We would use two encryption keys, the first key would be used to send this message "HI I am B", and the second key would be used for the following steps (the authentication protocol itself). If one key is cryptanalysis, the identity of the principal entity would still be preserved.

VI. Conclusion

In this paper, we presented a mutual authentication protocol which introduces the use of continued fractions in authentication schemes. We also improve the Needham-Schroeder-Lowe protocol by eliminating the identity of the principal in the authentication messages.

The rounding errors presents in the computation of the partial quotients could be an advantage, since the absence of agreement on the rounding errors between the principal and the intruder will

increase the probability of failure of any attack.

It could be interesting to see in the future, which properties of continued fractions may help to reduce the cost of partial quotients calculations.

Due the computer limitation, the use of irrational numbers can be theoretical, but as proved in [6], we can use an approximation of irrational numbers.

References

- [1] M. Beeler, R.W. Gosper, Schroepfel, R. Hakmen, "MIT Artificial intelligence memo 239", Feb. 29, 1972.
- [2] E.B. Burger, R. Tubbs, "Making transcendence transparent: An intuitive approach to classical transcendental number theory", Springer-Verlag, 2004.
- [3] M. Burrows, M. Abadi, R. Needham, "A logic of authentication", Technical Report 39, Digital Systems Research Center, 1989.
- [4] J. Clark, J. Jacob, "A survey of authentication protocol literature", 1997.
- [5] D. E. Denning, G. M. Sacco, "Timestamps in key distribution protocols", Communication of the ACM, 24(8), pp. 533-536, August 1981.
- [6] A. M. Kane, "On the use of Continued Fractions for Stream Ciphers", In Proceedings of Security and Management 2009, Las Vegas, USA.
- [7] A.M. Kane, "On the use of continued fractions for electronic cash", in International Journal of Computer Science and Security, Vol. 4, No. 1, pp. 136-148, 2010.
- [8] D. E. Knuth, "The art of computer programming Volume 2: Seminumerical algorithms (3rd Edition)", Addison-Wesley, 1997.
- [9] P. Levy, "Sur les lois de probabilité dont dépendent les quotients complets et incomplets d'une fraction Continue", Bull. Soc. Math. 57, 1929, pp. 178-194.
- [10] G. Lowe, "Breaking and Fixing the Needham-Schroeder Public-Key Protocol using FDR", in: Proc. TACAS'96, Springer LNCS 1055, 1996, pp. 147-166.
- [11] A.J. Menezes, P.C. van Oorschot, S.A. Vanstone, "Handbook of applied cryptography", CRC Press Series on Discrete Mathematics and its Applications. CRC Press, Boca Raton, FL, 1997.
- [12] R. Needham, M. Schroeder, "Using Encryption for Authentication in Large Networks of Computers", Comm. ACM 21 (12), 1978, pp. 993-999.
- [13] C. D. Olds, "Continued Fractions", Random House, 1963.
- [14] O. Perron, "Die Lehre Von Den Kettenbrüchen", 3rd ed. 1954.
- [15] B. Schneier, "Applied cryptography (2nd ed.): protocols, algorithms, and source code in C", John Wiley & Sons, Inc., 1995.
- [16] J. G. Steiner, B. C. Neuman, J. I. Schiller, "Kerberos: An authentication service for open network systems", In Proceedings of the Winter 1988 Usenix Conference, pp. 191-201, 1988.



V. Uma Maheswari, Assistant Professor, Department of Computer Science and Engineering, Vardhaman College of Engineering, Shamshabad, Hyderabad, AP, India



S. Anitha Reddy, Associate Professor, Department of Computer Science and Engineering, Krishna Murthy Institute of Technology and Engineering, Edulabad, Ghakesar, AP, India