Research Journal of Applied Sciences, Engineering and Technology 8(1): 131-134, 2014
DOI:10.19026/rjaset.8.950
ISSN: 2040-7459; e-ISSN: 2040-7467

Submitted: March 29, 2014 Accepted: April 28, 2014 Published: July 05, 2014

Research Article

Buchmann-Williams Authenticated Key Agreement Protocol With Pre-shared Password

Soufiane Mezroui, Abdelmalek Azizi and M'hammed Ziane
Laboratoire ACSA, Département de Mathématiques et Informatique, Université Mohammed Premier, Oujda 60000, Morocco

Abstract: Based on Buchmann-Williams key exchange protocol, a Buchmann-Williams Authenticated Key Agreement (BWAKA) protocol with pre-shared password is proposed. Its security relies on the Discrete Logarithm Problem over class groups of number fields. It provides identity authentication, perfect forward secrecy and key validation.

Keywords: Diffie-Hellman, reduced ideals, simple authenticated key agreement

INTRODUCTION

Two decades ago, Buchmann and Williams (1988) proposed a key exchange protocol based on Imaginary Quadratic fields (IQC). The security of this protocol rests on the discrete logarithm problem over the class groups of imaginary quadratic fields. The best known methods to solve this problem are exponential and sub-exponential under Riemann Hypotheses. Thus the strength-per-key-bit is substantially greater in (IQC) than that in conventional Discrete Logarithm (DL) systems and smaller parameters can be used in (IQC) but with equivalent levels of security. For example, (IQC) keys of about 687 bits are about equivalent in strength to RSA or DSA (Digital Signature Algorithm) keys of about 1024 bits, which is a significant saving. These advantages are especially important in environments where processing power, storage space, or power consumption is constrained.

Furthermore, Aydos *et al*. (1998) proposed an ECC based authentication and key agreement protocol for wireless communication. It makes use of Diffie-Hellman protocol and provides identity authentication and key validation. A trusted authority, named certificate authority, is incorporated and thus the user end is required to process certificates. Another method for achieving an authenticated key agreement protocol is to use a pre-shared secret password. SAKA algorithm, which is proposed by Seo and Sweeney (1999). Researchers have made many modifications to SAKA (Ku and Wang, 2000).

Combining the above two protocols with and elliptic curves authenticated key agreement with pre-shared password given by Aifen *et al*. (2005), a Buchmann-Williams Authenticated Key Agreement (BWAKA) protocol is proposed. The pre-shared password mechanism is used to lighten the computation and storage burden of the user equipment. The protocol is proved theoretically and the security features are analyzed.

BUCHMANN-WILLIAMS KEY EXCHANGE SYSTEM

This section recall briefly what is the Buchmann-Williams protocol. Let $D<0$ be a square free integer and let $K = Q(\sqrt{D})$ be the imaginary quadratic field. It is well known that the ring of algebraic integers O_K, of K is $Z + Z\omega$.
where,

$$\omega = (r - 1 + \sqrt{D})/r$$

and,

$$r = \begin{cases} 2 \; when \;\; D \equiv 1 (\mathrm{mod}\, 4), \\ 1 \; when \; D \equiv 2,3 (\mathrm{mod}\, 4) \end{cases}$$

Now if I is any ideal of O_K, then,

$$I = Za + Z(b + c\omega)$$

where, a, b, $c \in Z$, $a>0$, $c>0$, $c|a$, $c|b$ and $ac|N_{K/Q}(b+c\omega)$. We denote a by $L(I)$. The ideal I is called primitive when $c = 1$. Further, it is said to be reduced if it is primitive and there does not exist a nonzero $\beta \in I$ so that $|\beta| < |a|$.

It is well known that each equivalence class of ideals of O_K contains a reduced ideal. Indeed, there is an algorithm for finding such a reduced ideal.

Corresponding Author: Soufiane Mezroui, Laboratoire ACSA, Département de Mathématiques et Informatique, Université Mohammed Premier, Oujda 60000, Morocco

Algorithm:

- For a given primitive ideal $I = I_1 = Za + Z(b + \omega)$ of O_K, put $Q_0 = ra > 0$, $P_0 = r(b + \omega) - \sqrt{D} \in Z$. The value of r here is that defined above.
- Compute $q_i = Ne(P_i/Q_i)$, $P_{i+1} = q_iQ_i - P_i$, $Q_{i+1} = (P_{i+1}^2 - D)/Q_i$, where by $Ne(\gamma)$ we denote an integer such that $|\gamma - Ne(\gamma)| \leq 1/2$ which is unique unless $x = \pm 1/2$.
- $I_{i+1} = ZQ_i / r + Z\frac{P_i + \sqrt{D}}{r}$ is a reduced ideal of O_K when $Q_{i+1} \geq Q_i$.

This algorithm requires a polynomial running time. Indeed, one can find a reduced ideal at most after $2 + \frac{1}{2}\log_2(3\frac{Q_0}{5}\sqrt{|D|})$ steps.

Throughout the paper, for any ideal I of O_K, we note I_{red} to be the reduced ideal equivalent to I.

Now, we are able to describe the Buchmann-Williams protocol: Two users Alice and Bob select a value of D so that $|D|$ is large and an ideal I in O_K. The value of D and the ideal I are public:

- Alice selects at random an integer x and computes a reduced ideal J such that $J \sim I^x$. She sends J to Bob.
- Bob selects at random an integer y and computes a reduced ideal L such that $L \sim I^y$. He sends L to Alice.
- Alice computes a reduced ideal L^x_{red} equivalent to L^x; Bob computes a reduced ideal J^y_{red} equivalent to J^y.

Since $L^x \sim J^y \sim I^{xy}$, the reduced ideal computed by Alice and Bob is the same and so $L^x_{red} = J^y_{red}$. They can take as the common secret key $L(L^x_{red}) = L(J^y_{red})$.

AUTHENTICATED KEY AGREEMENT ALGORITHM

We recall the Simple Authenticated Key Agreement (SAKA), our presentation is largely inspired by Aifen *et al*. (2005). The main problem of the Diffie-Hellman key exchange method is that it is vulnerable to man-in-the-middle attacks. To solve this problem, user authentication is required by adopting certificates into a key exchange. Thus, Eve cannot impersonate Alice or Bob and cannot substitute the original public keys with her own because they are signed. One example of this scheme is the authenticated Diffie-Hellman key agreement protocol, or Station-to-Station (STS) protocol (Diffie *et al*., 1992). But the extension to a larger system may be difficult (Seo and Sweeney, 1999). They need a larger storage for certificates and more bandwidth for verification of the signature as the number of users increase. Furthermore, if the authority is compromised then the total system would be in danger.

Another kind of authenticated key exchange protocol assumes a pre-shared secret password between two users. Encrypted Key Exchange (Bellovin and Merritt, 1992) is a famous example. But it is complicated. The SAKA, which is also based on Diffie-Hellman protocol, requires only two packets to agree on the secret session key. The steps in the SAKA are described as follows. The system possesses two public values n and g as in the original Diffie-Hellman scheme.

Assume Alice and Bob share a secret password P before the protocol begins. Each computes two integers Q and Q-1 mod (n-1) from the password P. Q is computed in predetermined way from P and is prime to (n - 1), with low probability that two different passwords will give the same value of Q:

- Alice chooses a random large integer a and sends $X_1 = g^{aQ}$ mod n to Bob
- Bob chooses a random large integer b and sends $Y_1 = g^{bQ}$ mod n to Alice
- Alice computes $Y = Y_1^{Q-1}$ mod $n = g^b$ mod n, $K_A = Y^a$ mod $n = g^{ab}$ mod n
- Bob computes $X = X_1^{Q-1}$ mod $n = g^a$ mod n, $K_B = X^b$ mod $n = g^{ab}$ mod n

Key validation follows:

- Alice sends K^Q_A mod $n = g^{abQ}$ mod n to Bob
- Bob sends K^Q_B mod $n = g^{abQ}$ mod n to Alice
- Both Alice and Bob compute the other's key by applying Q^{-1} and compared with his/her own session key

The weakness of the SAKA is due to the same values of the two validation messages.

In the validation phase, Eve receives K^Q_A in 1 from Alice. Then Eve impersonates Bob to re-send K^Q_A to Alice. Now the validation in 3 is always correct. Though Eve cannot establish a session key with Alice, Alice is convinced that she has obtained a correct session key. Thus the protocol does not provide identity authentication.

Since the validation messages K^Q_A and K^Q_B are transmitted over the channel. When a password Q is compromised, the old session key K_B can be recovered using $(K^Q_B)^{Q-1}$ mod n.

Thus SAKA does not provide perfect forward secrecy. Though with the above disadvantages, SAKA is simple to be implemented. Based on SAKA, a Buchmann-Williams Authenticated Key Agreement (BWAKA) protocol is proposed to adapt to wireless

environments. The pre-shared password mechanism is adopted to lighten the computation and storage burden of the user's equipment.

BUCHMANN-WILLIAMS AUTHENTICATED KEY AGREEMENT PROTOCOL

Choosing a square free integer $D<0$ and the imaginary quadratic field $K = Q(\sqrt{D})$. Given any ideal I of O_K with the big order n in the class group of K.

Now, Alice and Bob share a secret password S. Individually, they compute two integers t and $-t$. t is derived from S in any predetermined way and it yields a unique value. The whole protocol is divided into two phases: Key establishment phase and validation phase.

Key establishment phase:

- Alice chooses a random integer $d_A \in [1, n-1]$, computes the reduced ideal Q_{Ared} equivalent to $Q_A = I^{d_A+t}$ and sends Q_{Ared} to Bob
- Bob chooses a random integer $d_B \in [1, n-1]$, computes the reduced ideal Q_{Bred} equivalent to $Q_B = I^{d_B+t}$ and sends Q_{Bred} to Alice
- Alice computes the reduced ideals X_{red}, K_{Ared} equivalents to $X = Q_B \times I^{-t} = I^{d_B}$ and $K_A = X^{d_A} = I^{d_A d_B}$ respectively
- Bob computes the reduced ideals Y_{red}, K_{Bred}, equivalents to $Y = Q_A \times I^{-t} = I^{d_A}$ and $K_B = Y^{d_B} = I^{d_A d_B}$

Key validation phase:

- Alice computes the reduced ideal ${K_A}^t{}_{red}$ equivalent to ${K_A}^t = I^{td_A d_B}$ and sends it to Bob
- Bob checks whether ${K_A}^t{}_{red} = {K_B}^t{}_{red}$ holds or not. If it does, Bob believes that he and Alice have obtained the same session key $K_{Ared} = K_{Bred}$. Since Bob knows d_B, he believes he has obtained the correct Q_{Ared}. Since Alice knows d_A, Bob believes Alice has obtained the correct Q_{Bred}. i.e., Bob is convinced that K_{Bred} is validated and sends the reduced ideal $I^{d_A t}{}_{red}$ equivalent to $I^{d_A t}$ to Alice
- Alice checks $I^{td_A}{}_{red}$. If $I^{td_A}{}_{red}$ is correct, Alice believes that Bob has obtained the correct Q_{Ared}. Since only Bob knows t besides Alice, Alice believes that she has obtained the correct Q_{Bred} and they have obtained the same session key $K_{Ared} = K_{Bred}$. Alice is convinced that K_{Ared} is validated

After the verification procedure has been completed by both sides, Alice and Bob are now ready to use the session key.

SECURITY ANALYSIS

Identity authentication: On the one hand, assuming Eve can impersonate Bob. When Eve receives Q_A, she sends the reduced ideal Q_{Ered} equivalent to $Q_E = I^d = I^{t+d_E}$ to Alice. But Eve does not know t and d_E and she cannot make the validation message $I^{td_A d_E}{}_{red}$, thus the key validation fails. On the other hand, with 2 and 3 of the key validation phase, Alice and Bob believe that only knowing t can generate the valid validation messages.

Man-in-the-middle attacks: In the original Diffie-Hellman protocol, Eve can alter the public values such as $g^a \bmod n$ or $g^b \bmod n$ with her own values. Thus Eve can share session keys with Alice or Bob. In our protocol, when Eve receives $Q_{A_{red}} = I^{d_A+t}{}_{red}$, she cannot guess d_A and t. If she tries to eavesdrop, she must generate $I^{d_E}{}_{red} = I^{d_A^*+t}{}_{red}$ and send it to Bob; Bob will obtain a wrong value $I^{d_A^* d_B}{}_{red}$, which is impossible for Eve to know. Thus Eve cannot share a session key with Bob or Alice.

Key validation: Through the key validation phase, Alice and Bob are convinced that they have obtained the same session key $I^{d_A d_B}{}_{red}$ and they are the only two to know the key.

Perfect forward secrecy: The messages transmitted over the channel include: $I^{d_A}{}_{red}$, $I^{d_B}{}_{red}$, $I^{td_A d_B}{}_{red}$ and $I^{td_B}{}_{red}$. Even if t (or the password S) is compromised, the random number d_A and d_B are still kept secret. Due to the difficulty in computing discrete logarithms over imaginary quadratic fields, no old session key can be recovered. Thus the protocol has the characteristics of perfect forward secrecy.

ACKNOWLEDGMENT

This study was supported by Académie Hassan 2 under the project "Mathématiques et Applications: cryptographie" and URAC6-CNRST.

REFERENCES

Aifen, S., L.C.K. Hui, Y. Yixian and K.P. Chow, 2005. Elliptic curves cryptography based authenticated key agreement with pre-shared password. J. Electron., 22: 268-272 (China).

Aydos, M., B. Sunar and C.K. Koc, 1998. An elliptic curve cryptography based authentication and key agreement protocol for wireless communication. Proceeding of the 2nd International Workshop on Discrete Algorithm and Methods for Model Computation and Communication. Dallos, Taxas.

Bellovin, S.M. and M. Merritt, 1992, Encrypted key exchange: Password-based protocols secure against dictionary attacks. Proceeding of the IEEE Computer Society Conference on Research in Security and Privacy. Oakland, California, pp: 72-84.

Buchmann, J. and H.C. Williams, 1988. A key-exchange system based on imaginary quadratic fields. J. Cryptol., 1: 107-118.

Diffie, W., P.C.V. Oorschot and M.J. Wiener, 1992. Authentication and authenticated key exchanges. Design Codes Cryptogr., 2: 107-125.

Ku, W.C. and S.D. Wang, 2000, Cryptanalysis of modified authenticated key agreement protocol. Electron. Lett., 36 (21): 1770-1771.

Seo, D.H. and P. Sweeney, 1999. Simple authenticated key agreement algorithm. Electron. Lett., 35(13): 1073-1074.