FULL SECURE KEY EXCHANGE AND AUTHENTICATION WITH NO PREVIOUSLY SHARED SECRETS

JOSEP DOMINGO i FERRER
LLORENÇ HUGUET i ROTGER

Dept. Informàtica
UNIVERSITAT AUTONOMA DE BARCELONA
08193 BELLATERRA

When speaking about secure networks, the bootstrapping process is very often forgotten or at least ignored. Some of the methods used so far do not protect against impersonation (Diffie-Hellman exponential key exchange) or have an important computational complexity (public-key based methods). A new algorithm is presented which is able to achieve key exchange whilst ensuring secrecy and authentication with a reasonable amount of computation.

1. INITIALIZATION

Let us define the necessary conditions for our system.

q, α are a large prime (say 150 digits), with q-1 having at least one large prime factor, and a primitive element of Z/(q), respectively, both publicly known. Each node i in the network has a very probably unique name (later we shall see what this means) in the form α^{ti} mod q where ti is chosen by i in the range 2..q-1 and only known to i. The node name is also publicly known and together with the other node names and α,q is available on all communication media (radio, television, newspapers and so on, what has been called the Merkle channel from Merkle's proposal). This latter assumption may look a little bizarre, but it is the only way to ensure that everybody in the network has access to the public information without any distortion.

J.J. Quisquater and J. Vandewalle (Eds.): Advances in Cryptology - EUROCRYPT '89, LNCS 434, pp. 665-669, 1990.
© Springer-Verlag Berlin Heidelberg 1990

To generate the public information listed in the previous paragraph, we can proceed as follows. A particular node i (it is only important that it be a single node, no matter which one), generates α, q and sends them over the Merkle channel, so that everybody can reliably learn these numbers. Then each node i generates a number ti in the range 2..q-1 and keeps it secret; then node i computes its name as α^{ti} mod q and sends it over the Merkle channel. Now every node knows α, q and each other's name. The probability for all nodes to have different names is

$$P(q-3,n)/PR(q-3,n),$$

where n is the number of nodes, P denotes permutations and PR permutations with repetition. It is trivial to see that this quantity approaches 1 if $q >> n^2$.

2. THE METHOD. NORMAL MODE: KEY EXCHANGE PROTOCOL

In what we call "normal mode", the presented method works as a **key exchange protocol providing secrecy and authentication**. After this mode has been used, the exchanged key can be used by this method in order either to encrypt and to decrypt messages, or to sign them, if some public parameters are added to those discussed in the previous section. Let us examine the "normal mode".

Node j first has α, q and knows all the node identifiers, in particular knows the identifier of node i, from which it wants to get a key, to be IDi = α^{ti} mod q. Of course, ti is only known to node i. Then node j and i proceed as follows:

STEP 1. NODE j: Compute X1, such that

$$gcd(X1,q-1) = 1 \quad \text{and} \quad 2 <= X1 <= q-2$$

Compute also $Y1 = \alpha^{X1} \bmod q$.
Send Y1 to NODE i.

STEP 2. NODE i: Upon receiving Y1, pick X2, X4 such that

[1] $X2 + X4 = ti \bmod (q-1)$ and $2 <= X2, X4 <= q-2$

Compute the key $K = \alpha^{X2} \bmod q$.
Compute $Y2 = Y1^{X2} \bmod q$.
Compute $Y4 = Y1^{X4} \bmod q$.
Send Y2 and Y4 to NODE j.

STEP 3. NODE j: Now NODE j computes the multiplicative inverse of X1 mod (q-1), $X1^{-1}$ such that

[2] $X1^{-1} * X1 = 1 \bmod (q-1)$

By computing

[3] $Y2^{X1^{-1}} \bmod q = K$

NODE j retrieves the key K it will share with NODE i from now on. An additional exponentiation yields

[4] $Y4^{X1^{-1}} \bmod q = \alpha^{X4} \bmod q$

In order to achieve authentication, NODE j performs the following test on K (if equation [5] does not hold, then the key K does not come from NODE i):

[5] $K * \alpha^{X4} \bmod q = IDi = \alpha^{ti} \bmod q$

END.

Now NODE i and NODE j share the key K which can be used either straightforwardly as a DES key (taking for example the 8 lower bytes of it), or act as a key-encrypting key to

transmit further keys, or be used as a key for the cryptosystem alternate mode of the presented method.

Note that some calculations **can be done in parallel** between NODE i and NODE j. For instance, NODE i can precalculate some (X2, X4) pairs for the next key transmissions to other nodes and can also precalculate the keys K it will send, in order to accelerate step 2. Also, while waiting for Y2, NODE j can compute $X1^{-1}$, so that step 3 is faster. A precalculation of some (X1, $X1^{-1}$, Y1) triples is also possible at node j. With all these improvements, only four interactive exponentiations are necessary:

- To compute Y2 at node i.
- To compute Y4 at node i.
- To retrieve K at node j.
- To retrieve α^{X4} mod q at node j.

This is equivalent to the four exponentiations required to ensure secrecy and authentication with RSA (two at NODE i and two at NODE j to retrieve the key), but it avoids the strong prime calculation (two strong primes per node).

3. FINAL REMARKS

Proofs of correctness, secrecy and authentication, as well as some extensions to the basic algorithm will be given in the full paper. It will be shown that this algorithm can work in an **alternate mode**, thus operating as a **unidirectional conventional** or as a **signature scheme.**

4. REFERENCES

[DDD85] R. A. DeMillo, G. I. Davida, D. P. Dobkin et al., Applied Cryptology, Cryptographic Protocols, and Computer

Security Models, Proc. of Sympsia in Applied Math., Vol 29, American Mathematical Society (1985).

[Den82] D. E. Denning, Cryptography and Data Security, Addison-Wesley 1982.

[DH88] J. Domingo, L. Huguet, "Secure network bootstrapping: an algorithm for authentic key exchange and public-key encryption", IEEE Transactions on Information Theory (submitted).

[Diff88] W. Diffie, "The First Ten Years of Public-Key Cryptography", Proc. of the IEEE, Vol 76. No. 5, May 1988.

[FSh87] A. Fiat and A. Shamir, "How to prove yourself: Practical solutions to identification and signature problems", Crypto'86, Springer-Verlag (1987).

[GMR85] S. Goldwasser, S. Micali and C. Rackoff, "Knowledge complexity of interactive proofs", 17th Symposium on the Theory of Computing, 1985.

[HDP88] L. Huguet, J. Domingo and J. Ponsa, "Communications Cryptography: a DES-based System for PC's", Proc. of the MIMI'88, June 1988.

[RSA78] R. L. Rivest, A. Shamir and L. Adleman, "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems", Communications of the ACM, Feb. 1978

[Sim88] G. J. Simmons, "A Survey on Information Authentication", Proc. of the IEEE, Vol. 76, No.5, May 1988.