AN IDENTITY-BASED KEY-EXCHANGE PROTOCOL

Christoph G. Günther
Asea Brown Boveri
Corporate Research
CH-5405 Baden, Switzerland

ABSTRACT

The distribution of cryptographic keys has always been a major problem in applications with many users. Solutions were found for closed user groups and small open systems. These are, however, not efficient for large networks. We propose an identity-based approach to that problem which is simple and applicable to networks of arbitrary size. With the solution proposed, the user group can, furthermore, be extended at will. Each new user needs only to visit a key authentication center (KAC) once and is from then on able to exchange authenticated keys with each other user of the network. We expect this type of approach, which was originally conceived for authentication and signatures, to play an increasing role in the solution of all types of key distribution problems.

I. INTRODUCTION

The transmission of data at medium to high rate requires the use of symmetric encryption algorithms. The key distribution problem implied in this mode is frequently solved by using the Diffie-Hellman key-exchange algorithm [1] or some of its variants. A major concern in large networks is then the authentication of the public keys used in the algorithm. A local storage of this list requires a large storage capacity and is, in addition, inflexible with respect to network extensions. A centralised storage, on the other side, implies a communication complexity comparable to

J.J. Quisquater and J. Vandewalle (Eds.): Advances in Cryptology - EUROCRYPT '89, LNCS 434, pp. 29-37, 1990.

the communication complexity of classical key distribution protocols and therefore ruins the advantage of the scheme. The same situation occurs with the El-Gamal signature protocol [2].

Rivest, Shamir and Adleman [3] have indicated a solution to the problem of authenticating public keys: A key authentication center (KAC) signs the public key of each user and thereby guarantees its authenticity. The implementation of this solution for the authentication of the public keys used in the Diffie-Hellman scheme is typically not very practical. Fiat [4] has proposed an interesting approach to identification and signatures. In this approach the user of some communication facility only needs to know the "name" of his communication partner and the public key of the KAC. Such schemes are correspondingly called identity-based.

We adapt this approach for the construction of an identity-based key-exchange scheme (section III). In this protocol the two parties construct keys which agree if they are both legitimate and do both conform to the protocol. The actual authentication is established when the decryption of the message sent by the other party is meaningful. It is obvious that such a protocol cannot be zero-knowledge in the sense of Goldwasser, Micali and Rackoff [5] or Feige, Fiat and Shamir [6], since no simulator can construct the key in polynomial time if the encryption scheme is reasonable. Nevertheless, the protocol has some kind of zero-knowledge property, which will be discussed elsewhere. In section III we shall make some further remarks.

In the following, we assume that p is prime and we use the definition $\mathbf{Z}_m := \{0, 1, \ldots, m-1\}$ and $\mathrm{GF}^*(p) :=$ *the multiplicative group of* $\mathrm{GF}(p)$. Finally, $t \in_R \mathbf{Z}_{p-1}$ means t is chosen at random from $\mathbf{Z}_{p-1}$.

II. IDENTITY-BASED PROTOCOLS

Identity-based protocols were mainly considered for authentication and signature. Examples are given by Fiat and Shamir [7], Beth [8] and Guillou and Quisquater [9]. Identity-based protocols run in three phases: a set-up phase, a preauthentication phase and an authentication phase. The first two phases involve a key authentication center (KAC), which is trusted by all parties. The essence of the protocol can be summarised as follows: The set-up phase is used by the KAC to lay down all the system parameters. In the preauthentication phase all those who wish to join the network visit the KAC and identify themselves. Let Alice be such a user, then after verification of her identity the KAC forwards her the signature of her name and the system parameters. *The central property of identity-based protocols is that after completion of this preauthentication phase Alice is able to authenticate herself (authentication phase) to any other user without further communication with the KAC and without uncovering the secret signature of her name.* We would like to use such a protocol in order to authenticate the public key r^s used in the Diffie-Hellman scheme. The El-Gamal signature scheme [2] is, as we shall see, very well adapted to solve this and other authentication problems. The steps read as follows:

Set-up:
The KAC chooses a one-way function f, a finite field $\mathrm{GF}(p)$ in which it is difficult to compute discrete logarithms, a primitive element $\alpha \in \mathrm{GF}^*(p)$ and at random some number $x \in \mathbf{Z}_{p-1}$ which is not divisible by the largest prime factor of $p-1$. The number x is the KAC's private key. It is used to compute the public key $y = \alpha^x$.

Preauthentication:
Alice visits the KAC and identifies herself. If the KAC accepts her, it provides her with f, $\mathrm{GF}(p)$, α and y. Furthermore, it computes the El-Gamal signature (r, s) of $ID = f$(description of Alice), gives it to Alice and keeps it secret otherwise. The "description of Alice," D, may include Alice's name, birthday, physical description or whatever is suitable for the application intended. The one-way function f is used in order to increase the redundancy of D if the inherent redundancy is either too small or difficult to use. (A certain amount of redundancy is needed in order to avoid El-Gamal's attack 5 [2], *i.e.*, in order to avoid the generation of valid triples (ID, r, s).) The computation of the signature (r, s) runs as follows [2]: the KAC chooses at random $k \in \mathbf{Z}_{p-1}$, with $\gcd(k, p-1) = 1$, computes $r := \alpha^k$, and solves the equation $ID = xr + ks \bmod (p-1)$ for s. We note that no k should be used repeatedly, since this would uncover the secret key x. We also note that, due to the assumption $\gcd(k, p-1) = 1$, the element r is primitive.

Authentication:
The verification equation for the signature reads:

$$\alpha^{ID} = y^r r^s, \tag{1}$$

and can be rewritten in the form

$$r^s = \alpha^{ID} y^{-r}. \tag{2}$$

This equation leads to the following reinterpretation of the El-Gamal scheme: *It is a scheme for the computation of the discrete logarithm s to a primitive basis r of an expression that only depends on publicly known quantities and on the base r to which the logarithm is taken.*

We note that making r public does not compromise the secret key s, since determining a pair (r, s) which signs the message ID is at least as difficult if r is prescribed as it is when r can be chosen freely. The base r does also not need to be authenticated since the determination of a pair (r, s) is precisely breaking an instance of the El-Gamal signature scheme.

If Alice now wishes to authenticate herself, she uses the Chaum, Evertse, van de Graaf protocol [10] in order to "prove" in zero-knowledge that she knows s. This is Beth's identity-based zero-knowledge proof of identity [8].

In section III we shall consider a corresponding protocol for key-exchange. Here, we conclude by noting that the reinterpretation of equation (2) also leads to an identity-based El-Gamal signature scheme. If Alice wishes to sign a message $m \in \mathbf{Z}_{p-1}$, she chooses $\kappa \in \mathbf{Z}_{p-1}$ with $\gcd(\kappa, p-1) = 1$, determines $\rho = r^\kappa$ and computes σ by solving the equation $f(m) = s\rho + \kappa\sigma \bmod (p-1)$. The signature (ρ, σ) then satisfies the verification equation:

$$\begin{aligned} r^{f(m)} &= (r^s)^\rho \, \rho^\sigma \\ &= (\alpha^{ID} y^{-r})^\rho \, \rho^\sigma. \end{aligned} \tag{3}$$

In particular, Alice can act as a KAC for another user David, if she chooses $m = ID' = ID_{David}$, $\rho = r'$, $\sigma = s'$. In this way whole hierarchies of KAC's can be constructed. Proving the security of this scheme seems to be outside the scope of todays methods. It is closely related to the security of the El-Gamal scheme itself.

III. AUTHENTICATED KEY EXCHANGE

In section II we have seen how to authenticate a number r^s for which the KAC can compute the discrete logarithm s to the base r. It is natural to use this scheme to authenticate the public keys in the Diffie-Hellman scheme. There is, however, one additional step to do: The basis r and r' of any two parties must be different, since else two of them could coalesce and, by sharing their secret keys s and s', determine the KAC's secret key. The Diffie-Hellman algorithm must, therefore, be adapted to accommodate different basis for the parties. Incidentally, this adaption has the advantage to generate a different key at each session. The resulting protocol reads

Alice		Bob
Step 0:		
$y \in \mathrm{GF}^*(p)$		$y \in \mathrm{GF}^*(p)$
$r \in \mathrm{GF}^*(p)$		$r' \in \mathrm{GF}^*(p)$
$s \in \mathbf{Z}_{p-1}$		$s' \in \mathbf{Z}_{p-1}$
Step 1:		
	$\xrightarrow{D,\ r}$	
	$\xleftarrow[D',\ r']{}$	
$ID' = f(D')$		$ID = f(D)$
$r'^{s'} := \alpha^{ID'} y^{-r'}$		$r^s := \alpha^{ID} y^{-r}$
Step 2:		
$t \in_R \mathbf{Z}_{p-1}$		$t' \in_R \mathbf{Z}_{p-1}$
$u := r'^t$		$u' := r^{t'}$
	$\xrightarrow{u}$	
	$\xleftarrow[u']{}$	
Step 3:		
$z = u'^s$		$z = (r^s)^{t'}$
$z' = (r'^{s'})^t$		$z' = u^{s'}$
$\zeta = zz'$		$\zeta = zz'$

As stated in the introduction, this protocol cannot be zero-knowledge in the traditional sense. Let us, however, make two remarks to show that the protocol does not disclose much information on Alice's secret s and correspondingly on Bob's secret s'. Alice only sends two quantities to Bob. These are r and u:

- sending r gives no useful information to Bob or any other party. The reason is as follows: Bob or the other party can either break the El-Gamal scheme in which case they do not need to receive r, or they cannot break that scheme. In the latter case, they can, however, not determine s, since this would precisely mean to break an instance of the El-Gamal scheme with a prescribed r. (We note that not even the KAC is able to determine an s associated with an r of which it does not know the discrete logarithm.)
- u is uncorrelated to s.

In order to discuss the soundness, we assume that Clair wants to impersonate Alice. Then she has to determine ζ without knowing s. She can certainly determine z'. Her problem is to compute $z = r^{t's}$ from $r^{t'}$ and $r^s = \alpha^{ID}y^{-r}$. We expect this to be of a comparable difficulty as breaking the Diffie-Hellman scheme. Due to the lack of further results on the El-Gamal and the Diffie-Hellman scheme this can, however, not yet be proved.

Let us finally consider the following slight modification of the steps 2 and 3 of the protocol:

Step 2:

$$\begin{array}{lcr} t \in_R \mathbf{Z}_{p-1},\ u := r'^{t} & & t' \in_R \mathbf{Z}_{p-1},\ u' := r^{t'} \\ w \in_R \mathbf{Z}_{p-1},\ v := \alpha^{w} & & w' \in_R \mathbf{Z}_{p-1},\ v' := \alpha^{w'} \\ & \xrightarrow{u,\ v} & \\ & \xleftarrow[u',\ v']{} & \end{array}$$

Step 3:

$$\begin{array}{ccc} z = u'^{s} & & z = (r^{s})^{t'} \\ z' = (r'^{s'})^{t} & & z' = u^{s'} \\ \tilde{z} = v'^{w} & & \tilde{z} = v^{w'} \\ \zeta = zz'\tilde{z} & & \zeta = zz'\tilde{z} \end{array}$$

This modification restores a property of the Diffie-Hellman scheme, which we could call *perfect forward secrecy:* If Alice and Bob are not impersonated, when the protocol is run, finding the key ζ is as difficult as breaking the Diffie-Hellman scheme for *every* third party. We note that even the KAC could be the third party. This has the important consequence that if by accident the KAC's secret key becomes known, the confidentiality of past message would not be compromised. Only the authenticity in the future would be lost.

IV. RELATED WORK

Bauspieß and Knobloch [11] have obtained a key-exchange scheme very similar to the identity-based protocol of section III. In their protocol Alice and Bob first run Beth's zero-knowledge identification scheme once in each direction. Alice and Bob then use the commitments of the respective verifiers in these protocols (which are authenticated if the protocols end successfully) as inputs to two Diffie-Hellman key-exchanges. They thus end up with two keys, one authenticated by Bob and the other one by Alice, which they could then suitably combine. Their protocol has the property of perfect forward secrecy from the beginning but is somewhat more involved than ours. The great advantage of the approach chosen by Bauspieß and Knobloch is, however, that the soundness of their protocol only depends on the security of the El-Gamal and of the Diffie-Hellman schemes, taken separately.

At the conference, we learned about a result of Okamoto and Tanaka, which has appeared in the mean time [12]. Okamoto and Tanaka transform the Diffie-Hellman key-exchange scheme into an identity-based one by using the RSA-scheme [3] as a trap-door function for the computation of the discrete logarithm of the ID-number. Their scheme uses only one data-exchange and is very attractive, due to its low communication complexity. It is, however, not perfectly forward secure. The introduction of that property would require to leave the ring $\mathbf{Z}_n$ $(n = p \cdot q)$ with some part of the protocol. Unfortunately, the security of the protocol seems also difficult to assess.

V. CONCLUSION

The authenticated key-exchange algorithm described in section III is simple and only needs few data exchanges. The security level only depends on the length of the words exchanged and not on the number of exchanges. The operations involved in the protocol are identical to those involved in a Diffie-Hellman key-exchange. The security could not be assessed within the current terminology, but some arguments were given why the scheme should be secure. We would thus expect that this type of protocols, including those of Okamoto and Tanaka [12], and Bauspieß and Knobloch [11], will play an increasing role for the security in large data systems.

REFERENCES

[1] W. Diffie, M.E. Hellman, "New Directions in Cryptography," *IEEE Trans. on Inform. Theory,* vol. IT-22, pp. 644-654, Nov. 1976.

[2] T. El-Gamal, "A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms," *IEEE Trans. on Inform. Theory,* vol. IT-31, pp. 469-472, July 1985.

[3] R.L. Rivest, A. Shamir, L. Adleman, "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems," *Comm. ACM,* vol. 21, pp. 120-126, Feb. 1978.

[4] A. Shamir, "Identity-Based Cryptosystems and Signature Schemes," *Advances in Cryptology - CRYPTO'84*, Lect. Notes in Computer Science, vol. 196, pp. 47-53, Springer-Verlag (1985).

[5] S. Goldwasser, S. Micali, C. Rackoff, "The Knowledge Complexity of Interactive Proof Systems," *SIAM J. Comput.*, vol. 18, pp. 186-208, Feb. 1989.

[6] U. Feige, A. Fiat, A. Shamir, "Zero-Knowledge Proofs of Identity," *J. of Cryptology,* vol. 1, pp. 77-94, 1988.

[7] A. Fiat, A. Shamir, "How to Prove Yourself: Practical Solutions to Identification and Signature Problems," *Advances in Cryptology - CRYPTO'86*, Lect. Notes in Computer Science, vol. 263, pp. 186-194, Springer-Verlag (1987).

[8] T. Beth, "Efficient Zero-Knowledge Identification Scheme for Smart Cards," *Advances in Cryptology - EUROCRYPT'88*, Lect. Notes in Computer Science, vol. 330, pp. 77-84, Springer-Verlag (1988).

[9] L.C. Guillou, J.-J. Quisquater, " A Practical Zero-Knowledge Protocol Fitted to Security Microprocessor Minimizing Both Transmission and Memory," *Advances in Cryptology - EUROCRYPT'88*, Lect. Notes in Computer Science, vol. 330, pp. 123-128, Springer-Verlag (1988).

[10] D. Chaum, J.-H. Evertse, J. van de Graaf, "An Improved Protocol for Demonstrating Possession of Discrete Logarithms and Some Generalizations," *Advances in Cryptology - EUROCRYPT'87*, Lect. Notes in Computer Science, vol. 304, pp. 127-141, Springer-Verlag (1988).

[11] F. Bauspieß, H.-J. Knobloch, "How to Keep Authenticity Alive in a Computer Network," *Advances in Cryptology - EUROCRYPT'89*, Lect. Notes in Computer Science, this issue, Springer Verlag.

[12] E. Okamoto, K. Tanaka, "Key Distribution System Based on Identification Information," *IEEE J. Select. Areas Commun.*, vol. SAC-7, pp. 481-485, May 1989.