Cryptanalysis of the Chang-Wu-Chen key distribution system

Mike Burmester

RH – University of London, Egham, Surrey TW20 OEX, U.K.

Abstract. Chang-Wu-Chen presented at Auscrypt 92 a conference key distribution system based on public keys. We show that this scheme is insecure and discuss ways to fix it.

1 The CWC key distribution system

This system [3] uses a discrete logarithm setting with prime modulus p and primitive element g. Each party U_j, $j = 1, 2, \ldots, n$, has a secret key $x_j \in Z_{p-1}$ and a public key $y_j = g^{x_j} \bmod p$. A chairperson U_0 with secret key $x_0 \in Z_{p-1}$ and public key $y_0 = g^{x_0} \bmod p$ picks a random $r \in Z_{p-1}$ and computes $Y = \prod_{i=1}^{n}(y_i)^r \bmod p$. The conference key is $k \equiv Y^{-1} (\bmod p)$. Then the chairperson sends each U_j: $c_1 = g^r \bmod p$, $c_2 = (y_0)^k \bmod p$, and $Y_j \equiv Y/(y_j)^r (\bmod p)$. The parties U_j can easily compute k, since $k \equiv (Y_j \cdot (c_1)^{x_j})^{-1} (\bmod p)$. To validate k, U_j checks that $c_2 = (y_0)^k \bmod p$.

2 A cryptanalytic attack

We have

$$\prod_{i=1}^{n} Y_i \equiv \prod_{i=1}^{n} (Y/(y_i)^r) \equiv Y^{n-1} \equiv k^{1-n} \ (\bmod p) .$$

So a passive eavesdropper can easily compute $k^{n-1} \bmod p$. Since it is feasible [7, 1] to compute $(n-1)$–th roots in Z_p, the eavesdropper will succeed in finding the key k (with non-negligible probability) when $n \geq 2$.[1]

3 Authentication

In a key distribution system each party should know with whom it is exchanging the key. With the CWC system it is clear that the chairperson can substitute some of the parties $U_1, U_2, \ldots, U_n$ without the others finding this out from the key distribution system. So it is essential that the parties trust the chairperson. However the chairperson U_0 is not authenticated. Indeed the secret key x_0 of U_0 is not needed to compute either the validator c_2, or any of c_1, Y_j and the key k. So anyone can easily masquerade as U_0 (by substituting its messages).

[1] Edward Zuk from Telecom Research Laboratories, Australia, has found this attack independently. This was pointed out to me by Jennifer Seberry.

T. Helleseth (Ed.): Advances in Cryptology - EUROCRYPT '93, LNCS 765, pp. 440-442, 1994.

4 Fixing the system

4.1 Using a prime modulus

We get some protection from the attack in Section 2 by replacing Y and Y_j by $\tilde{Y} \equiv (y_0)^{r(n-1)} \cdot \prod_{i=1}^{n} (y_i)^r \pmod{p}$ and $\tilde{Y}_j \equiv \tilde{Y}/(y_j)^r \pmod{p}$ respectively, and by taking $\tilde{k} \equiv \tilde{Y}^{-1} \pmod{p}$ as the key.

Consider a variant of the CWC system for which the chairperson U_0 sends U_j *only* c_1 and $\tilde{Y}_j$, and *not* c_2 which, as observed earlier does not authenticate U_0 (in this case U_0 must be authenticated some other way – see Section 4.3). We shall show that cracking this variant by a passive eavesdropper (a 'ciphertext attack') is as hard as cracking the Diffie-Hellman [6] problem,

Input: g, p, $g^a \bmod p$, $g^b \bmod p$; **Output:** $g^{ab} \bmod p$.

Indeed suppose that it is easy to crack the modified key distribution system and let $g^a \bmod p$, $g^b \bmod p$ be an instance of the Diffie-Hellman problem. Set $c_1 = g^a \bmod p$, $y_0 = g^b \bmod p$ and $y_i = g^{t_i - b} \bmod p$, for $i = 1, 2, \ldots, n$, where the $t_i \in Z_{p-1}$ are chosen randomly. Then $g^r \equiv g^a \pmod{p}$ and $\tilde{Y}_j \equiv (g^a)^{T-t_j} \pmod{p}$, where $T = \sum_{i=1}^{n} t_i$. We are assuming that it is easy to compute the key,

$$\tilde{k} \equiv \tilde{Y}^{-1} \equiv (g^b)^{a(1-n)} \cdot g^{a(nb-T)} \equiv g^{ab-aT} \pmod{p},$$

so it is easy to compute $g^{ab} \equiv \tilde{k} \cdot (g^a)^T \pmod{p}$, and hence to find a solution for the Diffie-Hellman problem. The reduction in the reverse direction is straightforward: if it is easy to crack the Diffie-Hellman problem, then it is easy to compute $\tilde{k} \equiv ((y_0)^{n-1} \cdot \prod_{i=1}^{n} y_i)^{-r} \pmod{p}$, from $(y_0)^{n-1} \cdot \prod_{i=1}^{n} y_i \pmod{p}$ and $g^{-r} \bmod p$.

For this variant of the CWC system we also get some protection from known key attacks ('plaintext attacks') by active adversaries. This follows by observing that 'old-session' information: $c_1 = g^r \bmod p$, $\tilde{Y}_j \equiv ({y_0}^{n-1} \cdot \prod_{i \neq j} y_i)^r \pmod{p}$, and $\tilde{k} \equiv \left({y_0}^{n-1} \cdot \prod_{i=1}^{n} y_i\right)^r \pmod{p}$, can be simulated, and that therefore the argument used in [8] for 'non-paradoxical' systems applies. However it should be pointed out that there is a flaw [5] in the proof given in [8], and consequently the proposed variant *may* not be 'proven secure' for known key attacks (in the general case).

4.2 Using a composite modulus

To prevent the attack in Section 2 we may also use a composite modulus $m = pq$, where p, q are appropriate primes, and take g to be an element of large order, e.g. a primitive element of Z_p and Z_q.[1] Then it is not necessary to modify Y and Y_j. For a 'provably secure' protocol we may use the variant in the previous section with composite modulus (however in this case the probability distributions are not uniform and we must use randomized reductions [2] as in [8]). Again we get some protection from known key attacks.

4.3 Addressing the authentication problem

As pointed out in Section 3 the validator c_2 does not authenticate the chairperson U_0, since anybody can compute it without knowing the secret key x_0. To prevent this we may replace c_2 by $\tilde{c}_{2j} = (y_j)^{\tilde{k}x_0} \bmod p$. Clearly it is hard to compute $\tilde{c}_{2j}$ without knowing $\tilde{k}$ and either x_0 or x_j, provided the Diffie-Hellman problem is hard. Furthermore any U_j can easily validate $\tilde{k}$, since $\tilde{c}_{2j} \equiv (y_0)^{\tilde{k}x_j} \pmod p$. However this modification offers no protection against insider attacks. Indeed any U_i can compute $(y_j)^{x_0} \equiv (y_0)^{x_j} \pmod p$ from $\tilde{c}_{2j}$ (obtained by eavesdropping) and from the key $\tilde{k}$ [7, 1]. Then, at any later time, U_i can impersonate U_0, or forge any key $\tilde{k}$.

There seems to be no obvious way of solving the authentication problem without using a separate authentication system. The scheme in [4] addresses this problem and other more general issues.

Acknowledgement. The author wishes to thank Yvo Desmedt and Dieter Gollmann for many helpful discussions.

References

1. L. Adleman, K.M. Manders, and G.M. Miller. On taking roots in finite fields. *Annual Symposium on Foundations of Computer Science*, Vol. 18, 1977, pp. 175–178.
2. S. Ben-David, B. Chor, O. Goldreich, M. Luby. On the theory of Average case Complexity. *Proceedings of the twenty first annual ACM Symp. Theory of Computing, STOC*, 1977, pp. 175–178.
3. Chin-Chen Chang, Tzong-Chen Wu, and C.P. Chen. The Design of a Conference Key Distribution System. Presented at Auscrypt 92, Gold Coast, Australia, December 13-16, 1992. To appear in: *Advances in Cryptology, Lecture Notes in Computer Science*, Springer-Verlag.
4. M. Burmester, Y. Desmedt. An Efficient and Secure Conference Key Distribution System. Manuscript, April 1993.
5. Y. Desmedt, M. Burmester. Towards practical 'proven secure' authenticated key distribution. To appear in, Proceedings of the 1st ACM Conference on Communications and Computing Security, Fairfax, Virginia, November 3–5, 1993.
6. W. Diffie and M. E. Hellman. New directions in cryptography. *IEEE Trans. Inform. Theory*, IT–22(6), 1976, pp. 644–654.
7. D. Shanks. Five number theoretic algorithms. *Proc. Second Manitoba Conf. Numerical Mathematics*, 1972, pp. 51–70.
8. Y. Yacobi. A Key Distribution Paradox. In *Advances in Cryptology — Crypto '90, Proceedings (Lecture Notes in Computer Science #537)*, 1991, A.J. Menezes and S.A. Vanstone, Eds, Springer-Verlag, pp. 268–273.