Access control at the Netherlands Postal and Telecommunication Services

Haemers, W.H.

Published in:
Advances in cryptology-CRYPTO '85

Publication date:
1986

ACCESS CONTROL AT THE NETHERLANDS POSTAL AND TELECOMMUNICATIONS SERVICES

Willem Haemers
PTT, Dr Neher Laboratories
Leidschendam, The Netherlands

Abstract. The Netherlands Postal and Telecommunications Services (PTT) have developed a system that controles the entrance to their buildings by use of magnetic stripe cards. In this note some cryptographic aspects of the system are explained.

The Netherlands PTT has about 100,000 employees and 2,000 buildings. Many of the employees have access to several buildings. The access control system provides each employee with only one magnetic stripe card, irrespective of the number of buildings the employee has access to. Because of the complexity of the situation an off-line system is prefered. It implies that the access information must be on the magnetic stripe card. The access information consists of the following subjects:

- identity of the employee
- buildings to which the employee has access
- times when access is allowed
- access under special circumstances
- PIN-code
- random information

For reasons of security and organisation it is required that the card distribution center only is able to create cards. This is achieved by encrypting the information by means of a public key system. The secret encryption key, needed to create cards, is then only present at the center, whilst the public decryption key, needed to interpret the cards is present in each building. This kind of public key application can be found in [1] p. 512, and in [3].

Decryption is required to be implemented in PASCAL on a micro computer. A straightforward implementation of RSA takes about one minute. For decoding, this is much too long. Waiting at the entrance should not take more than half a second. One can speed up the decryption of RSA by use of a small exponent. However, Rabin [2] provides a system that in all cases is faster than RSA. The decryption formula for Rabin's system reads

(*) $\quad$ (clear text) = (cipher text)^2 MOD (public key),

where, as in RSA, public key is the product of two large primes. Computation of this formula has been realized in about 300 ms (the number size is 480 bits). Encoding still takes about one minute, but this is no problem.

After a card is read at the entrance the card holder can be asked to identify himself by means of a PIN. The PIN is a number chosen by the card owner and has no prescribed length. The information necessary for PIN checking, the PIN-code, is also on the card. If the PIN is typed at the entrance, the PIN-code is computed and compared with the PIN-code on the card. The PIN-code depends on the PIN and the identity of the card owner via a one-way function. The one-way function used is Rabin's decoding formula (*) (only 32 bits of the outcome are taken for the actual PIN-code).

It is impossible to prevent an exhaustive search attack on the PIN by anyone who knows the public key. Therefore the public key is not made public. However, it is straightforward to derive the public key from the plaintext and the ciphertext of about two cards. Therefor knowledge of the full plaintext is prevented by means of the random information on the card. The random information also prevents a chosen

plaintext attack which is known to exist for the used application of Rabin's system.

REFERENCES

[1] Meyer, C.H. & Matyas, S.M., "Cryptography: A New Dimension in Computer Data Security", John Wiley & Sons Inc., New-York, 1982.
[2] Rabin, M.O., "Digitalized Signatures and Public-Key Functions as Intractable as Factorization", MIT/LCS/TR-212 (1979).
[3] Simmons, G.J., "A System for Point-of-Sale or Access, User Authentication and Identification", Proc. Crypto '82, Santa Barbara, pp. 31-37.