Title: **Enforcing the security of a time-bound hierarchical key assignment scheme**

Authors: **De Santis A., Ferrara A.L. & Masucci B.**

Published in: *Information Sciences* 176(2006), no. **6**, 1684–1694

Review by: Mario Forcinito

The problem of time-bounded access control over distributed information or computational resources, has very important practical applications including Digital Rights Management and the access to databases containing sensitive commercial and industrial information.

Chien[1] proposed a time-bound hierarchical key assignment scheme based on tamper-resistant devices, that greatly reduces computation load and implementation costs. The authors and others[2] have written about Chien's scheme insecurity against a collusion attack. In this attack three users successfully conspire to access some secret keys belonging to a class for which they should not have access. This weakness stems from the way in which Chien's scheme allowed users to handle public and private information without proper authentication.

De Santis et al. propose three countermeasures that, without changing the nature of the operations performed by the tamper-resistant device or the Trusted Authority, can be used to strengthen Chien's scheme against collusion attacks.

These countermeasures involve additional hashing operations, encryption-decryption operations and authentication of the public information. Although in all cases there is an additional computation time penalty, these countermeasures are a preferred alternative to issuing a new tamper-resistance device to each class every time the keys are updated.

1. Chien H., *Efficient time-bound Hierarchical key assignment scheme*, IEEE Transactions on Knowledge and Data Engineering, vol. 16, no. 10, pp. 1301-1304, 2004.

2. Xun Yi, *Security of Chien's Efficient Time-Bound Hierarchical Key*

Assignment Scheme, IEEE Transactions on Knowledge and Data Engineering, vol. 17, no. 9, pp. 1298-1299, Sept., 2005.