Software Protection Using "Communal-Key-Cryptosystems"

G. Purdy Math. Dept. Texas A&M University
G. Simmons Sandia Labs Albuquerque NM
J. Studier Urbana Illinois

Abstract

We propose a method for software protection and distribution using tamper resistant modules (SECURE INFORMATION STORES) to achieve the following goals:

1. All encrypted copies of the software being distributed are identical, greatly reducing the cost of distribution.
2. The copy is accompanied by a key which enables only that software to run on only that machine.
3. No directories are needed.
4. Any software vendor can join the system without receiving privileged information.