ABSTRACT

Key management from a security viewpoint

G. R. Blakley

Department of Mathematics
Texas A&M University
College Station, Texas 77843

An information protection system (also called key safeguarding scheme, threshold scheme, secret sharing or key sharing) enables a protector of a piece of information S (called a substance) to use a large random input, coupled with the substance itself, to produce n + 1 pieces T(0), T(1), ..., T(n) of information (called shadows of the substance S) in a useful way. A threshold information protection system (TIPS) has the property that it is computationally trivial to recover S from any b + 1 shadows T(x(0)), T(x(1)), ..., T(x(b)) and impossible--in a precisely definable sense--to recover S from any b shadows T(y(1)), T(y(2)), ..., T(y(b)). A hysteresis information protection system (HIPS) has the property that more and more information about S is revealed by knowledge of more and more shadows. Some HIPS are very like TIPS.

The security proofs for TIPS demonstrate perfect security in the Shannon sense, rather than mere computational security. They require measure theory or content theory and involve some nontrivial probabilistic considerations. There are TIPS with infinitely many substances and shadows, suggesting, by analogy, the possibility of cryptosystems with infinite plaintext message spaces.

It is possible that all known TIPS, including the TIPS which has the Vernam one-time pad as a special case, are instances of a single very general ideal-theoretic description of a TIPS. Applications of TIPS to cryptography, as well as to various practical problems of information storage, are numerous. A few examples will be given, time permitting.