Security Mechanism in Electronic Cards

Stephen B. Weinstein
American Express Company
New York, N.Y.

Abstract

An "electronic card" may be broadly interpreted as any personally-carried access or payment medium which interfaces with electronic systems. This collection of cards includes those with magnetic stripes and magnetic watermarks, fluorescent codes, digital optical data storage and encpsulated semiconductor chips. Because they are used to obtain value of one sort or another, there is always the danger of fraud.

The fraud problems reviewed here fall into two major categories:

Unauthorized use of an authorized card, and use of a forged card. They depend heavily on whether use is at attended stations or unattended stations, and whether the station is on line to a data base or is offline. For online stations, both attended and unattended, the card can be (although it frequently is not) used only for convenience of data entry, leaving the real security mechanism to the bearer's interaction with the computer, which can involve passwords or physiological derivatives such as compressed signatures, fingerprints and voiceprints. The security of a card becomes a significant problem at offline stations where the granting of value depends on the bearer's relationship to his card.

For offline situations, elementary scrambling mechanisms afford some protection but have weaknesses against a serious attack. The inntelligent card with encpsulated semiconductor circuits and a password or physiological attribute utilization protocol has the potential for very high security, but as presently conceived is vulnerable to forgery attack.

This talk is a discussion of electronic systems and their security problems, introducing a practical field for applications of cryptographv and related securitv technology. Work is particularly needed on techniques which offer security against both card misuse and card forgery at unattended offline stations.