About this paper

The Protection of Information in Computer Systems

JEROME H. SALTZER, SENIOR MEMBER, IEEE, AND
MICHAEL D. SCHROEDER, MEMBER, IEEE

Invited Paper

Abstract *- This tutorial paper explores the mechanics of protecting computer-stored information from unauthorized use or modification. It concentrates on those architectural structures--whether hardware or software--that are necessary to support information protection. The paper develops in three main sections. Section I describes desired functions, design principles, and examples of elementary protection and authentication mechanisms. Any reader familiar with computers should find the first section to be reasonably accessible. Section II requires some familiarity with descriptor-based computer architecture. It examines in depth the principles of modern protection architectures and the relation between capability systems and access control list systems, and ends with a brief analysis of protected subsystems and protected objects. The reader who is dismayed by either the prerequisites or the level of detail in the second section may wish to skip to Section III, which reviews the state of the art and current research projects and provides suggestions for further reading.*

Glossary

The following glossary provides, for reference, brief definitions for several terms as used in this paper in the context of protecting information in computers.

Access

> The ability to make use of information stored in a computer system. Used frequently as a verb, to the horror of grammarians.

Access control list

> A list of principals that are authorized to have access to some object.

Authenticate

> To verify the identity of a person (or other agent external to the protection system) making a request.

Authorize

To grant a principal access to certain information.

Capability

In a computer system, an unforgeable ticket, which when presented can be taken as incontestable proof that the presenter is authorized to have access to the object named in the ticket.

Certify

To check the accuracy, correctness, and completeness of a security or protection mechanism.

Complete isolation

A protection system that separates principals into compartments between which no flow of information or control is possible.

Confinement

Allowing a borrowed program to have access to data, while ensuring that the program cannot release the information.

Descriptor

A protected value which is (or leads to) the physical address of some protected object.

Discretionary

(In contrast with *nondiscretionary*.) Controls on access to an object that may be changed by the creator of the object.

Domain

The set of objects that currently may be directly accessed by a principal.

Encipherment

The (usually) reversible scrambling of data according to a secret transformation key, so as to make it safe for transmission or storage in a physically unprotected environment.

Grant

To authorize (*q. v.*).

Hierarchical control

> Referring to ability to change authorization, a scheme in which the record of each authorization is controlled by another authorization, resulting in a hierarchical tree of authorizations.

List-oriented

> Used to describe a protection system in which each protected object has a list of authorized principals.

Password

> A secret character string used to authenticate the claimed identity of an individual.

Permission

> A particular form of allowed access, e.g., permission to READ as contrasted with permission to WRITE.

Prescript

> A rule that must be followed before access to an object is permitted, thereby introducing an opportunity for human judgment about the need for access, so that abuse of the access is discouraged.

Principal

> The entity in a computer system to which authorizations are granted; thus the unit of accountability in a computer system.

Privacy

> The ability of an individual (or organization) to decide whether, when, and to whom personal (or organizational) information is released.

Propagation

> When a principal, having been authorized access to some object, in turn authorizes access to another principal.

Protected object

A data structure whose existence is known, but whose internal organization is not accessible, except by invoking the protected subsystem (*q.v.*) that manages it.

Protected subsystem

A collection of procedures and data objects that is encapsulated in a domain of its own so that the internal structure of a data object is accessible only to the procedures of the protected subsystem and the procedures may be called only at designated domain entry points.

Protection

1) Security (*q.v.*).
2) Used more narrowly to denote mechanisms and techniques that control the access of executing programs to stored information.

Protection group

A principal that may be used by several different individuals.

Revoke

To take away previously authorized access from some principal.

Security

With respect to information processing systems, used to denote mechanisms and techniques that control who may use or modify the computer or the information stored in it.

Self control

Referring to ability to change authorization, a scheme in which each authorization contains within it the specification of which principals may change it.

Ticket-oriented

Used to describe a protection system in which each principal maintains a list of unforgeable bit patterns, called tickets, one for each object the principal is authorized to have access.

User

Used imprecisely to refer to the individual who is accountable for some identifiable set of activities in a computer system.
