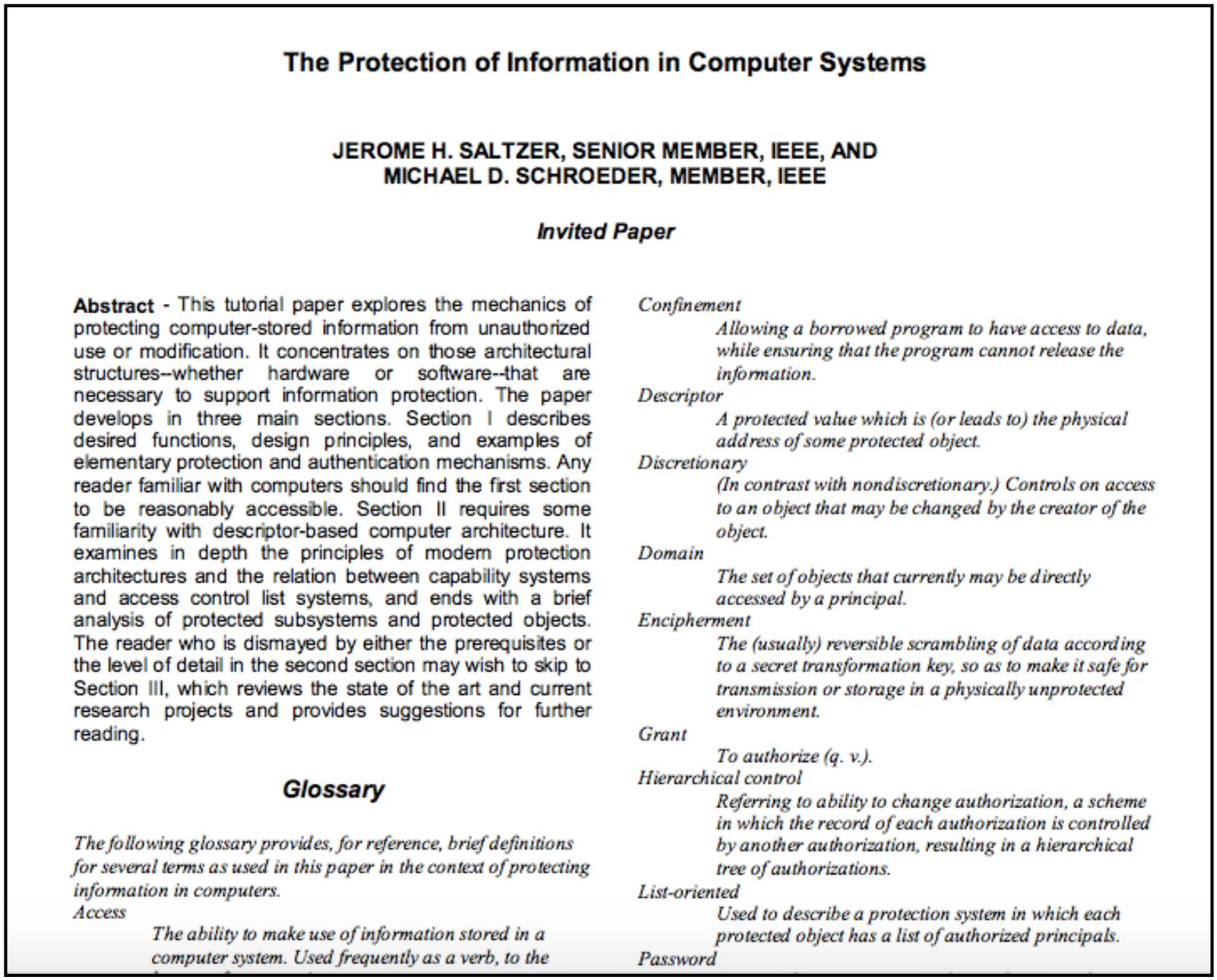
Security Principles

Yan Huang



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*

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

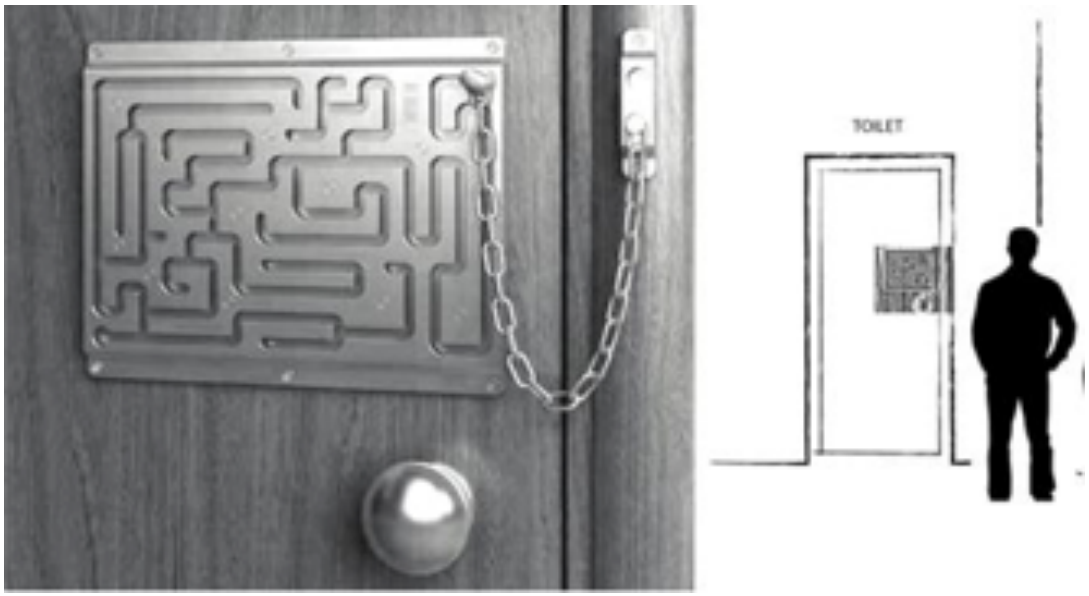
The Protection of Information in Computer Systems, Seltzer and Schroeder, Proceedings of IEEE, 1975

1. Economy of mechanism
2. Fail-safe defaults
3. Complete mediation
4. Open design
5. Separation of privilege
6. Least privilege
7. Least common mechanism
8. Psychological acceptability

Economy of Mechanism

Complexity is the enemy of security.

Economy of Mechanism



KISS — Keep It Simple, Stupid

Fail-safe Defaults

- Fail open: defaults to allow access
- Fail close: defaults to deny access
- Fail-safe: what is “safer”?

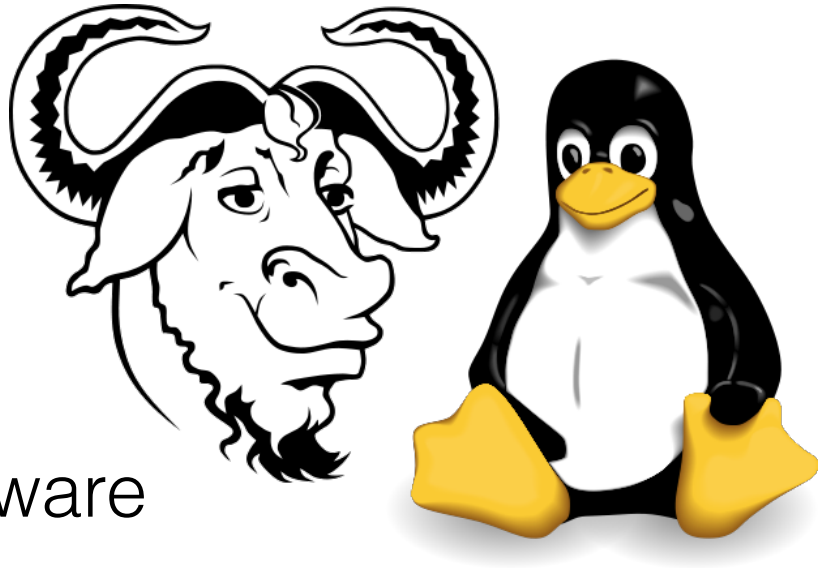
Complete Mediation

All accesses must be validated for authorization.

Complete Mediation

Open Design

Auguste Kerckhoffs



Opensource software

The mechanisms should not depend on the ignorance of potential attackers, but rather on the possession of specific, more easily protected, keys or passwords

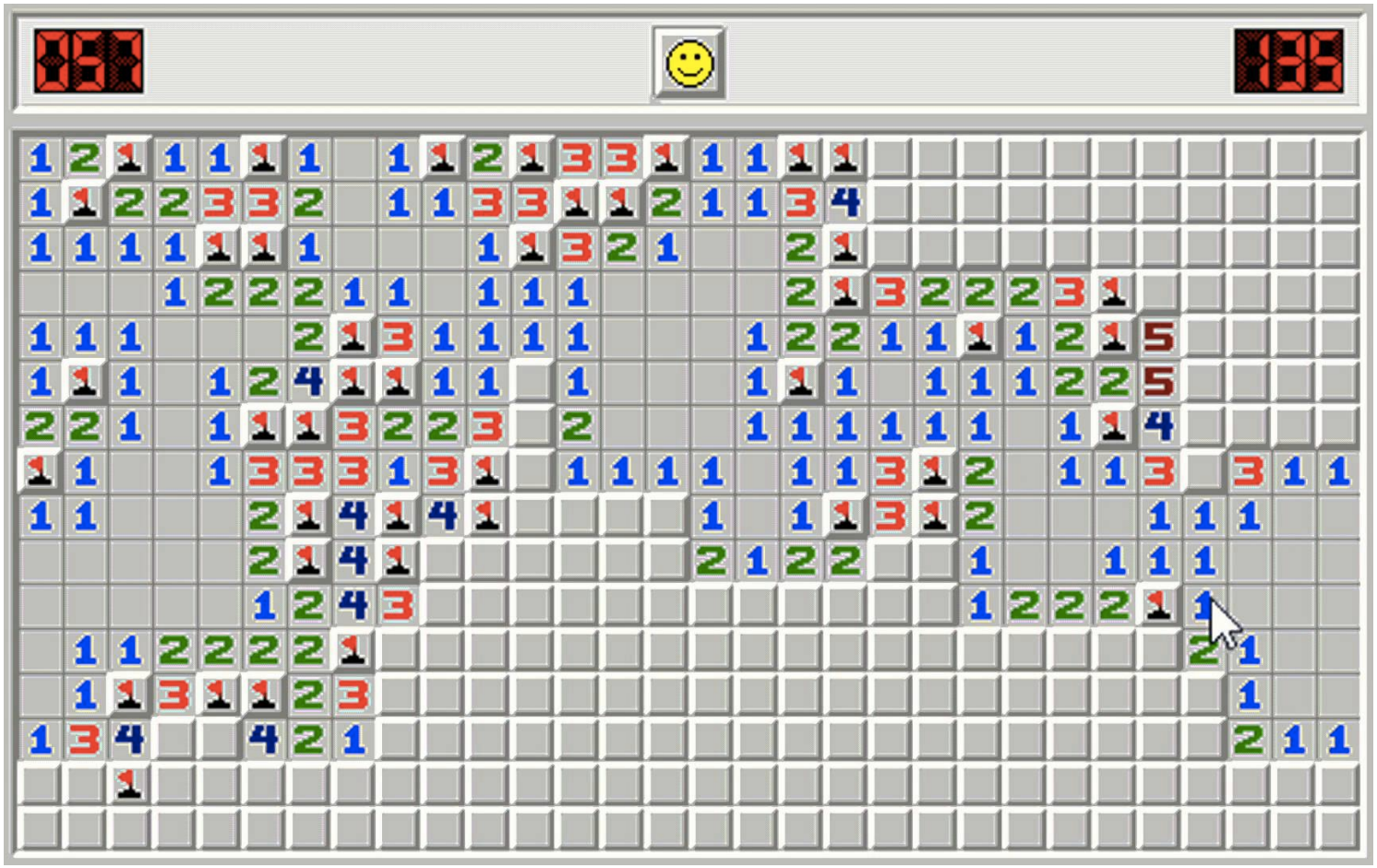
Separation of Privilege

A system requires two keys to grant access is more secure than that requires only one.

Least Privilege

Only grant permissions that are needed to complete the task

Least Privilege

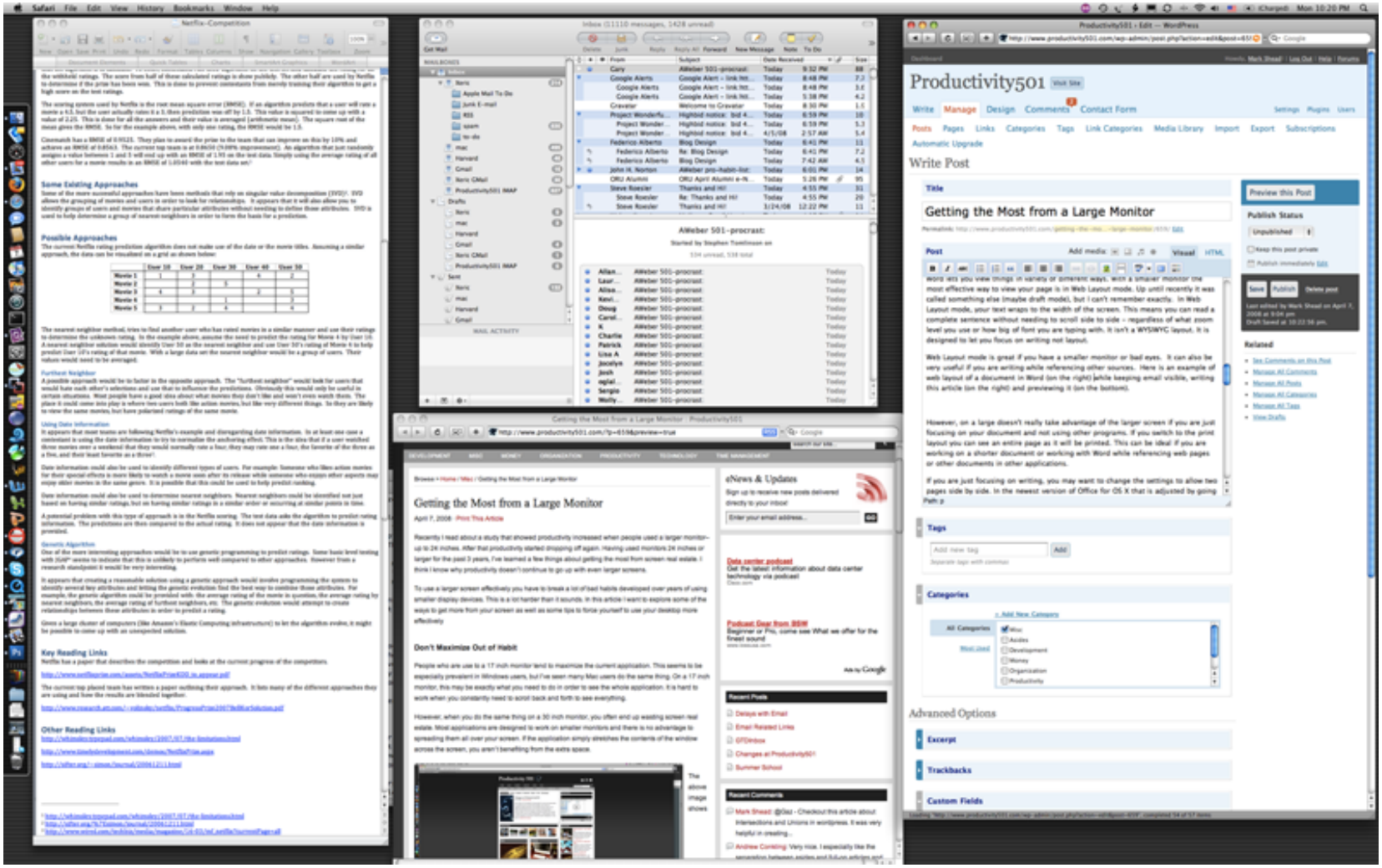


This program can also wipe out your hard drive.

Least Common Mechanism

Minimize the amount of mechanism common to more than one user and depended on by all (more) users.

Least Common Mechanism



Defend in Depth

Use layered defense mechanism that requires multiple types of successful attacks to penetrate.

Defend in Depth

Summary

1. Economy of mechanism
2. Fail-safe defaults
3. Complete mediation
4. Open design
5. Separation of privilege
6. Least privilege
7. Least common mechanism
8. Psychological acceptability

Charge

- Identify a paper of your interest from one of the top 4 security conferences in 2015: NDSS, IEEE Security and Privacy, USENIX Security, ACM CCS. Read the paper as much as you can answer the following questions:

    1. What is the title of the paper?

    2. What is the security problem?

    3. What are some potential (high level) solutions to the problem?

    4. What do the problem and its solutions have to do with the security principles we talked about today?

Bring it to class and hand in before class on Wednesday.