Protecting Data—The State of the Art

J. Saltzer
M. I. T.
OVERVIEW:

Two Approaches -

- PRAGMATIC
  
  Very useful
  
  High risk

- FORMAL
  
  Not yet ready
  
  Promises lower risk
Source of Risk: Error

Errors in:
- Specification
- Design
- Implementation
- Operation

No systematic way to exclude these errors

(proven by "Tiger teams")
The Problem: What does "Correct" Mean for Protection?

Addition:

A + B → A+B

Protection:

1. No formal model exists
2. Exhaustive test works
3. Tests inconclusive
INFORMAL SEMANTICS I

AUTHENTICATION (WHO IS THAT?)

EACH USER HAS ① DISTINCT NAME

② PASSWORD
OR
BADGE
OR
ENCIPHER KEY

CURRENT STATE:

HIGH QUALITY TECHNIQUES AVAILABLE
AREA QUITE WELL UNDERSTOOD
INFORMAL SEMANTICS II

**AUTHORIZATION (Joe may use this)**

- To authorize, one user must know other's name unambiguously

- Two approaches
  - Access control list
    - Easy to understand
    - Auditable
    - Revocation easy
  - Capability
    - Very efficient
    - Hardware can support

- Controls access to the data container, does not control use of the data
CURRENT STATE

- TOO EASY FOR USER TO MAKE MISTAKES

- CONTROL OF WHO MAY AUTHORIZE IS SUBJECT OF DEBATE
INFORMAL SEMANTICS III

LIMITED-USE SYSTEMS

- DEDICATE TO ONE APPLICATION
- NO USER-WRITTEN PROGRAMS
- INQUIRY-RESPONSE ONLY

CURRENT STATE:

- DEBATE OVER SAFETY
- SAFETY ← USER FLEXIBILITY

TRADEOFF NOT UNDERSTOOD
INFORMAL SEMANTICS IV

PROTECTED SUBSYSTEMS

CURRENT STATE:

- RESEARCH IMPLEMENTATIONS

- SOME CONNECTION WITH TYPE-EXTENSION

- PROBABLY USEFUL, BUT NOT YET PROVEN
FORMAL SEMANTICS

ONLY ONE COMPLETE MODEL:
- SENSITIVITY LEVELS
- COMPARTMENTS
- CONTROLS INFORMATION FLOW

MUST IDENTIFY EVERY OBSERVABLE
RESULT OF A PROGRAM EXECUTION

CURRENT STATE:
- RESEARCH AREA
- MODEL TOO RESTRICTED
- UNPROVEN BUT PROMISING
Problem Areas

- Formal Models of Other Policies
- Protection of Small Objects
- Statistical Inference
- How to Verify Compliance

Formal Model

System Specification

Implementation
Conclusion

Do not overestimate technical capability to protect information!