PROTECTING DATA-

THE STATE

OF THE

ART

J. SALTZER

M. I. T.

OVERVIEW:

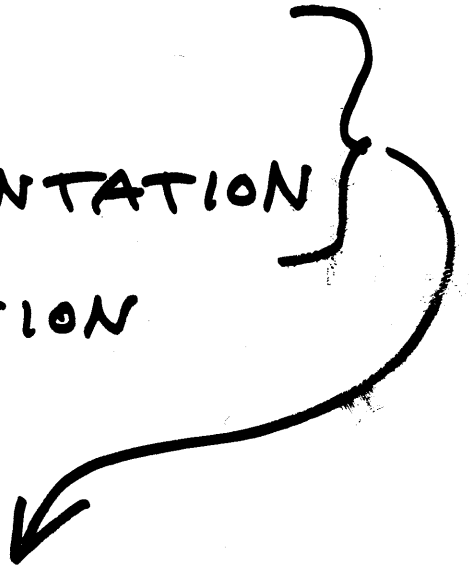
TWO APPROACHES -

- PRAGMATIC
  - VERY USEFUL
  - HIGH RISK
- FORMAL
  - NOT YET READY
  - PROMISES LOWER RISK

SOURCE OF RISK: ERROR

ERRORS IN:

- SPECIFICATION
- DESIGN
- IMPLEMENTATION
- OPERATION

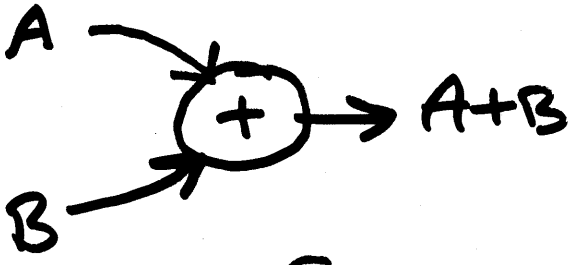


NO SYSTEMATIC WAY
TO EXCLUDE
THESE ERRORS

(PROVEN BY "TIGER TEAMS")

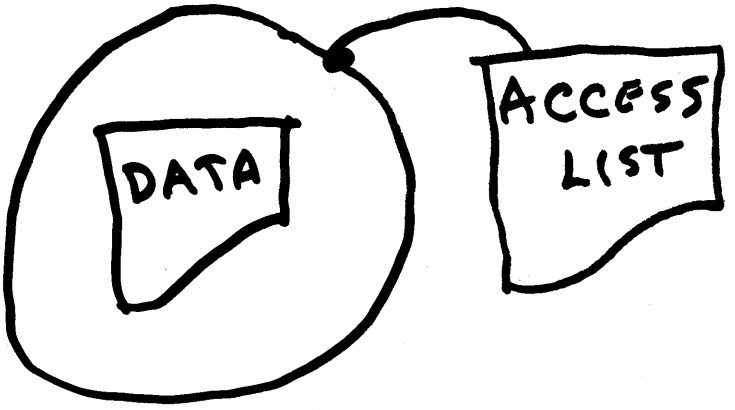
THE PROBLEM: WHAT DOES "CORRECT" MEAN FOR PROTECTION?

ADDITION:



① FORMAL MODEL EXISTS
② EXHAUSTIVE TEST WORKS

PROTECTION:



① NO FORMAL MODEL
② 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

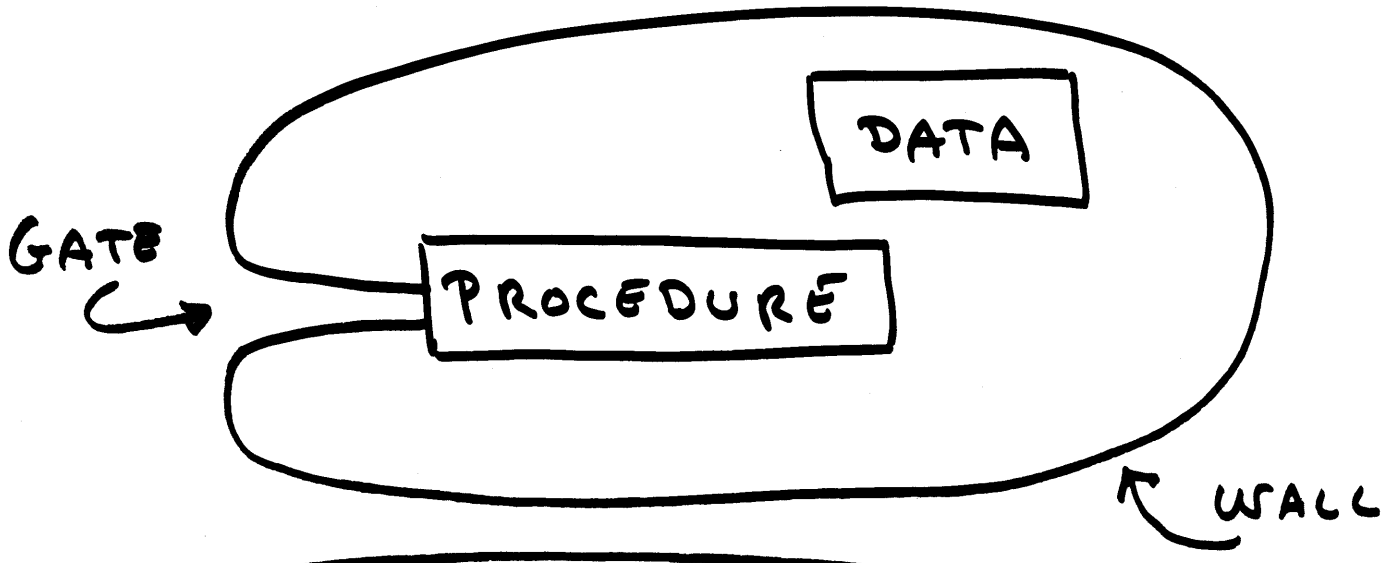
CURRENT STATE:

- 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

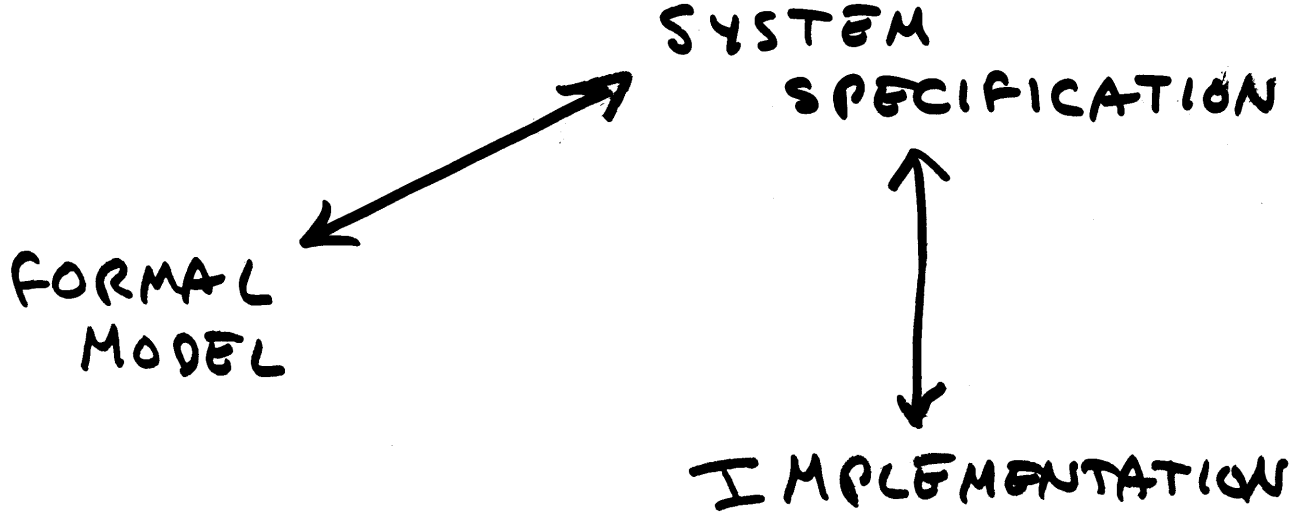
MUST IDENTIFY EVERY OBSERVABLE RESULT OF A PROGRAM EXECUTION

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



Conclusion

Do Not

Overestimate

Technical

Capability to

Protect Information!