CURRENT RESEARCH ON INFORMATION PROTECTION
Why is it "HOT"?

- Gov't Data Banks
  \[\rightarrow\]
  Consumer Interest

- IBM said so

- Military is worried

- Equity Funding (?)
INTEREST

$\quad$

22 "Big" Projects
13 "Little" Projects

~ 100 Professionals
**"Big" Projects:**

<table>
<thead>
<tr>
<th>CARNEGIE CAMBRIDGE</th>
<th>IBM RESEARCH SYSTEM DEVELOPMENT CORP.</th>
</tr>
</thead>
<tbody>
<tr>
<td>LAWRENCE R.L.</td>
<td>AIR FORCE ESD</td>
</tr>
<tr>
<td>ISI (USC)</td>
<td>NITRE</td>
</tr>
<tr>
<td>SRI</td>
<td>RAND</td>
</tr>
<tr>
<td>CASE</td>
<td>RUTGERS</td>
</tr>
<tr>
<td>OBERPFAFFENHUTEN</td>
<td>TRW SYSTEMS</td>
</tr>
<tr>
<td>U.C., BERKELEY</td>
<td>NBS</td>
</tr>
<tr>
<td>CORNELL</td>
<td>HISI</td>
</tr>
<tr>
<td>IBM / R.S.S.</td>
<td>MIT PROJECT MAC</td>
</tr>
<tr>
<td>UCLA</td>
<td>U. OF HAWAIJLL</td>
</tr>
</tbody>
</table>
What are all these people doing?

3 ASPECTS:

- Isolation
  Simple goal, but want perfection

- Access Control
  What semantics?
  Simplify interfaces

- "Advanced" ideas
  Extendible types
  Mutual suspicion
Research Problems

1. Architectural Capability vs. Access Control List

2. Interface Reducing Complexity

3. Implementation Proving Correctness

4. Network End-to-End Encryption
Major Current Projects

1. Architectural
   
   CMU: HYDRA
   
   CAMBRIDGE: CAP
   
   BERKELEY: PRIME

   CAPABILITIES
   
   THE EXTENSION
   
   PROVABLE
   
   CAPABILITIES
   USER INTERFACE
   
   SUPER RELIABLE
   DOUBLE CHECK
   ON PROTECTION
| **AF/ESD** | **MODEL THE GOVT SECURITY SYSTEM** |
| **NITRE** | **SECURE A PDP-11/45 OP SYSTEM** |
| **UCLA** | **MODEL VIRTUAL MACHINES** |
| **SRI** | **DIJKSTRA AT 13 LEVELS** |
| **ISI** | **PROVE PARALLEL PROGRAMS CORRECT** |
| **CASE** | **MODEL A FILE SYSTEM** |
| **HISI** | **SECURE MULTICS** |
| **M.I.T.** | **SIMPLIFY MULTICS** |
Get the simple partitions perfect

AF/ESD
MITRE
UCLA
SRI
ISI
CASE
HISI
M.I.T.

Model the Gov't Security System
Secure a POP-11/45 OP System
Model virtual machines
Dijkstra at 13 levels
Prove parallel programs correct
Model a file system
Secure MULTICS
Simplify MULTICS
Tiger Teams

ISI
Anderson, Inc.
LLL/RISOS
ESD
IBM Research
SDC

OS/360
R.S.S.
VM/370
WWMCCS
MULTICS
EVERYTHING, SOME DAY

Results
1. Case Studies (Secret)
2. Patterns
OTHER WORK

- SRI: Case studies of computer-based anti-social acts
- Berkeley: Security costs
- Cornell: Database controls (semantics)
- IBM Research: Encryption
- IBM SDO: User reaction to security
- RAND: Information theoretic aspects
- HISI: Secure I/O, networks
- Ohio State: Database controls
- Hawaii: Securing ILLIAC IV
Further Information

"Ongoing Research and Development on Information Protection",

ACM Operating Systems Review [SIGOPS Quarterly],

July, 1974