Paul Ashley Karger

Main Contributions

- Multics
  - Multics security enhancements, Multics vulnerability analysis
- Access Control
  - Non-Discretionary Access Control for Decentralized Computing Systems, Capability based Systems
  - Smart Card OS (embedded system) Access Control Model
- Virtualization
  - High performance, high assurance VMM for VAX
  - Requirements for virtualization, proposing the I/O-MMU (1975)
- Assurance
  - Evaluation techniques for high-assurance

… and many more

Some Publications

- Multics Security Evaluation: Vulnerability Analysis, June 1974, ESD-TR-74-193, Vol. 2, Hanscom AFB
  (together with Roger Schell)
  - Thirty Years Later: Lessons from the Multics Security Evaluation, 18th ACSAC
- Non-Discretionary Access Control for Decentralized Computing Systems, May 1977, MIT/LCS/TR-179
- Improving Security and Performance for Capability Systems, Ph.D Thesis, University of Cambridge, March 30, 1988
- A Retrospective of the VAX VMM Security Kernel, IEEE Transactions on Software Engineering, 1991
  (together with Mary Ellen Zurko, Douglas W. Bonin, Andrew H. Mason, and Clifford E. Kahn)
- Multi-Level Security Requirements for Hypervisors
- Authenticating Mandatory Access Controls and Preserving Privacy for a High-Assurance Smart Card, ESORICS 2003
  (together with H. Scherzer, R. Canetti, H. Krawczyk, T. Rabin, D. C. Toll)
- Increased Information Flow Needs for High-Assurance Composite Evaluations, 2nd IEEE Workshop on Information Assurance, 2004

This is just a short sample list. Look at the bibliography of each publication to find more

Quote

The internal controls of current computers repeatedly have been shown insecure through numerous Penetration exercises…. This insecurity is a fundamental weakness of contemporary operating systems and cannot be corrected by "patches", "fix-ups", or "add-ons" to those systems.

Rather, a fundamental reimplementation using an integrated hardware/software design which considers security as a fundamental requirement is necessary. In particular, steps must be taken to ensure the correctness of the security related portions of the operating system. It is not sufficient to use a team of experts to "test" the security controls of a system. Such a "tiger team" can only show the existence of vulnerabilities but cannot prove their non-existence.

From the Multics Vulnerability Analysis, 1974