

## Manuel Blum

<http://www.cs.cmu.edu/~mblum>

Manuel Blum, the Bruce Nelson University Professor of Computer Science at Carnegie Mellon University, is a pioneer in the field of theoretical computer science and the winner of the 1995 Turing Award in recognition of his contributions to the foundations of computational complexity theory and its applications to cryptography and program checking, a mathematical approach to writing programs that check their work.

He was born in Caracas, Venezuela, where his parents settled after fleeing Europe in the 1930s, and came to the United States in the mid-1950s to study at the Massachusetts Institute of Technology. While studying electrical engineering, he pursued his desire to understand thinking and brains by working in the neurophysiology laboratory of Dr. Warren S. McCulloch and Walter Pitts, then concentrated on mathematical logic and recursion theory for the insight it gave him on brains and thinking. He did his doctoral work under the supervision of Artificial Intelligence pioneer Marvin Minsky, and earned a Ph.D. from MIT in mathematics in 1964.

Blum began his teaching career at MIT as an assistant professor of mathematics and, in 1968, joined the faculty of the University of California at Berkeley as tenured associate professor of Electrical Engineering and Computer Sciences. He was Associate Chair for Computer Science, 1977-1980. He was named Arthur J. Chick Professor of Computer Science in 1995. Blum accepted his present position at Carnegie Mellon in 2001.

The problems he has tackled in his long career include, among others, methods for measuring the intrinsic complexity of problems. Blum's Speedup theorem is an important proposition about the complexity of computable functions. The Blum axioms give a machine-independent way to understand the complexity of computation, whether that computation is done by human or by computer. Since his early work on the intrinsic limitations of computing devices, Blum's research has focused on the single unifying theme of finding positive, practical consequences of living in a world where computational resources are bounded. In his work, Blum has shown that secure business transactions, pseudo-random number generation, program checking, and more recently, CAPTCHAs for detecting bot intruders, are possible in part because all computational devices are resource bounded.

Blum's current research includes the HumanOID (Human Oriented ID) project, a cryptographic project designed to develop a challenge-response authentication protocol that humans can perform entirely in their heads. For this, people must be able to authenticate themselves to a system while a powerful machine-based adversary that knows the protocol listens on the line and records every challenge and response. The system would have to be incapable of learning to impersonate that human.

A member of the National Academy of Sciences and the National Academy of Engineering, he is a fellow of the American Academy of Arts and Sciences, the American Association for the Advancement of Science, and the Institute of Electrical and Electronics Engineers. Dr. Blum has held a Sloan Foundation Fellowship and received a University of California at Berkeley Distinguished Teaching Award, their Faculty Research Award, the Sigma Xi's Monie A. Ferst Award, the Carnegie Mellon Herbert A. Simons Teaching Award, among other honors. He is the author of more than 50 papers published in leading scientific journals and has supervised the theses of 35 doctoral students who now pepper almost every major computer science department in the country. The many ground-breaking areas of theoretical computer science chartered by his academic descendants are legend.