Much of our computing infrastructure is still built using C and C++, in spite of overwhelming language-level problems that lead to security exploits. I will discuss a range of compiler-oriented techniques that researchers have explored to try and harden C/C++ code. In one corner, we have techniques such as Software Fault Isolation (SFI) that have low overhead, and guarantee to enforce a particular security policy. However, the SFI policy is relatively coarse-grained, and as such doesn’t block important attack classes. In another corner of the space is the Secure Virtual Architecture (SVA) which enforces a fine-grained, object-level integrity policy comparable to type safety. However, SVA and related techniques can have high overhead for some code, and will generally break more programs than SFI. All of these techniques depend upon compiler transformations, optimizations, and/or analyses that could lead to a large trusted computing base (TCB). So I will also discuss recent research that helps to minimize the TCB via machine-checked proofs of correctness.

Biography

Greg Morrisett received his B.S. in Mathematics and Computer Science from the University of Richmond, and his Ph.D. from Carnegie Mellon. He served on the Cornell CS faculty from 1996 to 2004, and then moved to Harvard as the Allen B. Cutting Professor of Computer Science. He served in the position of Associate Dean for Computer Science and Engineering from 2007-2010, and currently heads the Harvard Center for Research on Computation and Society. Morrisett has received a number of awards for his research on programming languages, type systems, and software security, including a Presidential Early Career Award for Scientists and Engineers, an IBM Faculty Fellowship, an NSF Career Award, and an Alfred P. Sloan Fellowship. He served as Chief Editor for the Journal of Functional Programming and as an associate editor for ACM Transactions on Programming Languages and Systems and Information Processing Letters. He currently serves on the editorial board for The Journal of the ACM and as co-editor-in-chief for the Research Highlights column of Communications of the ACM. In addition, Morrisett has served on the DARPA Information Science and Technology Study (ISAT) Group, the NSF Computer and Information Science and Engineering (CISE) Advisory Council, Microsoft Research’s Technical Advisory Board, Microsoft’s Trustworthy Computing Academic Advisory Board, and the CRA Board.