

=====
Steve Zdancewic

Title: Security-oriented Languages

Abstract:

It is well known that buffer overflow account for majority of security incidents that occur on the Internet today. Modern programming languages offer an appealing and practical solution to this problem through a combination of static analysis (type checking) and dynamic enforcement (array bounds checks). But buffer overflows are only one aspect of system security; once they have been dealt with, other higher-level security concerns such as authentication, access control, data confidentiality, and auditing become the focus.

This talk will look at how programming languages features can be designed to make it easier to specify and enforce security policies, particularly those dealing with access control and data confidentiality. The approach is to use augmented type systems that incorporate programmer-specified security policies that are checked at compile time. One challenge in this area is how to integrate language-based security with other existing security mechanisms such as the OS access controls or cryptographic protocols.