Topic Overviews

17-939A
Software Analysis, Security for SE

Vahe Poladian

Software Analysis - 1

> The Problem
  • Does the design of a system capture the intended purpose?
  • Does the code conform to the design?
  • Can we verify code for correctness? Partial correctness?
  • What abstractions do we need to analyze design and code?
  • What tools do we need to automate the analysis?

> A Definition
  • “The extraction of behavioral information from the software, represented as an abstract model or code” – Jackson, Rinard

> The Beginnings
  • 1945, first bug, a moth, found by Grace Hopper in ENIAC,
  • 1968, NATO Conference:
    – the problem of “exponential growth of errors” recognized,
    – acceptable threshold for errors per line of code discusses,
Software Analysis - 2

> The State of The Art
  • Analysis of models
    – model checking: (near)-exhaustive search of the state space,
    – theorem proving: expressing the statement of the program in logic
  • Analysis of code
    – static and dynamic,
    – sound and unsound,
    – issues: multi-threaded programs, distributed systems,

> The Future
  • Bridge the gap between model and source code,
  • Allow for incremental and modular analysis,
  • Consider cost, analyze only partially what matters most,
  • Improve precise, sound analysis for infrastructural software.

Security for SE - 1

> The Problem
  • Manage and distribute digital information securely,
  • Ensure that software systems comply with laws of governments and regulations of commerce,
  • Educate user communities about security and the possible risks resulting from lack or failure of security,

> The Milestones
  • Willis H. Ware, late 1960s, a pioneer in security and privacy,
  • Mandatory access controls, 1970s, formulation of security policies,
  • RSA, 1980s, strong cryptographic means for securing data,
  • Security protocols popularized in internet applications, 1990s,
Security for SE - 2

> The State of the Art in the Industry
  • Security protocols in widespread use; perimeter security;
  • Managed security emerging; insurance;
  • Security perceived as an economic value added;
  • Security for pervasive devices; faster cryptographic algorithms;

> … and Research Directions for The Future
  • Integrate security considerations early into life-cycle; apply cost-benefit analysis to allocate resources for security requirements,
  • Integrate security into legacy systems as they present weak links,
  • Improve software copy-protection and watermarking techniques,
  • Implement techniques for formulating desired security properties and develop tools for evaluating the security of systems,
  • Develop automated infrastructure for post-deployment of systems,