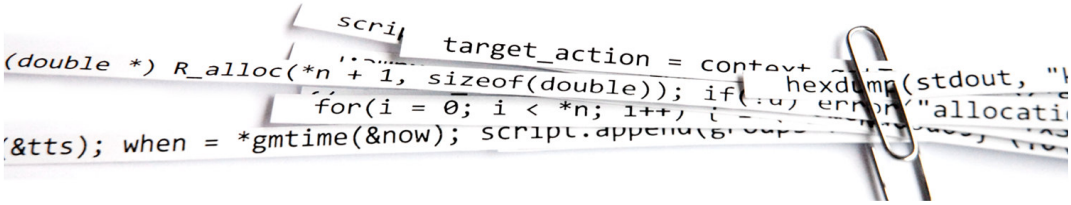
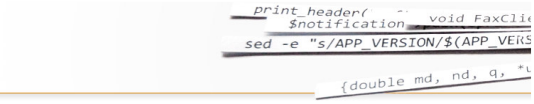
Source Code Quality and Security

Klocwork

Tony Czarnik



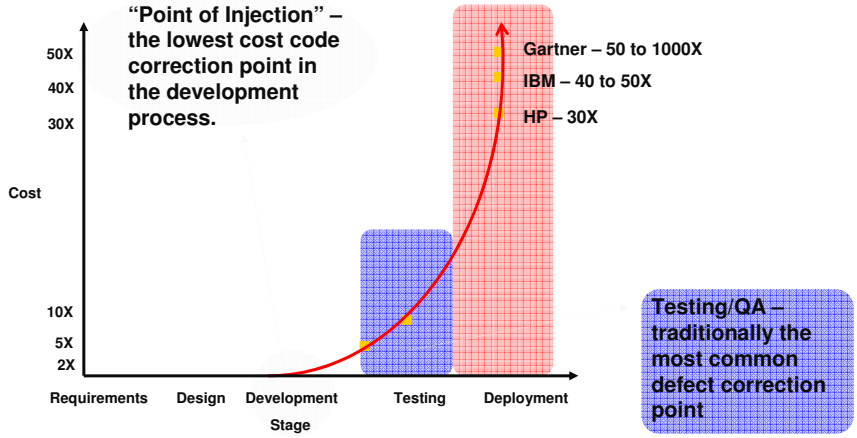
Agenda



- Quality & security: issues & trends
  - » Traditional testing limitations
- Source code analysis (SCA) tools
  - » First and second generation tools
  - » Third generation tools
    - CMMI in-phase containment
- National security standards
- Architectural analysis use cases
- Source code metrics & trending
- SCA tool integration
- Case study: Motorola

Static Source Code Analysis

- Problems with traditional testing techniques
  - » Black box; dynamic; functional testing: incomplete
  - » Walkthrus: time-intensive & incomplete

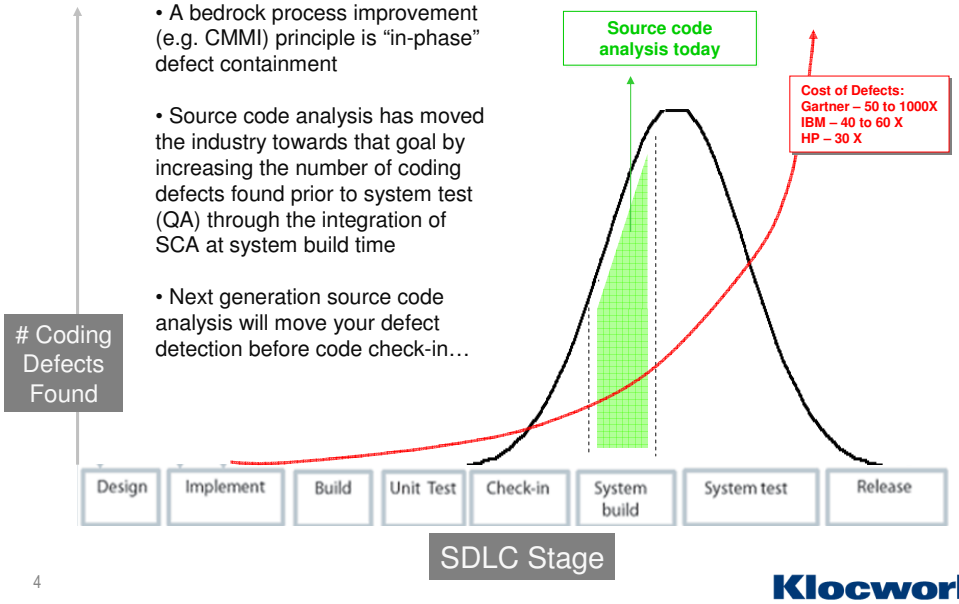


- Solution: Static source code analysis; white box testing

Klocwork

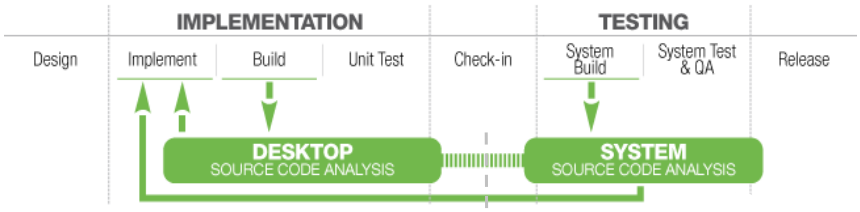
Source Code Analysis Today

- A bedrock process improvement (e.g. CMMI) principle is "in-phase" defect containment
- Source code analysis has moved the industry towards that goal by increasing the number of coding defects found prior to system test (QA) through the integration of SCA at system build time
- Next generation source code analysis will move your defect detection before code check-in…



Klocwork

Enabling the developer – accurate local analysis



Developer SCA - Benefits

- Reported problems can be fixed right away by the developer before it impacts anyone else
- Enables "in-phase" defect containment

Developer SCA – Limitations

- Accuracy problems if a developer runs only a few files without full system context
- Developers can't communicate changes/updates to defects they're reviewing

System SCA - Benefits

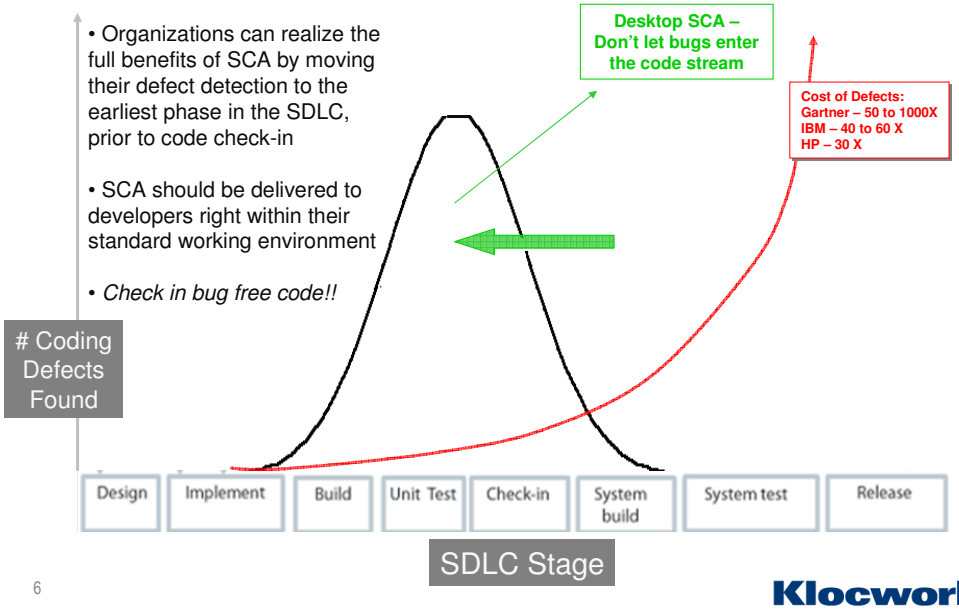
- Required for good analysis accuracy due to "whole system" visibility
- Essential for management and build over build reporting on quality trends

Systems SCA – Limitations

- Doesn't enable "in-phase defect containment" – developers have to check-in broken code to find out its broken
- Developers still caught in a "rinse and repeat" bug finding/fix/check-in cycle

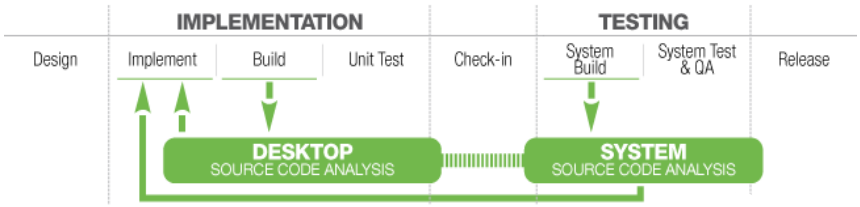
Klocwork

True In-Phase Defect Containment



Klocwork

Enabling the developer – accurate local analysis



- SCA developer desktop is automatically connected with system analysis
  - » Best performance, best accuracy, full system context delivered locally
  - » Creates peer-to-peer collaboration on bug resolution
  - » Defect "fingerprint" allows defect ID and developer actions to stay with the defect, ensuring developers don't duplicate work on same bug
  - » Integrated within IDE, or available via simple command line
- Combines the productivity benefits of desktop source code analysis with the power and accuracy of system-wide analysis
- Supports Agile Development

Klocwork

Source code quality defects

- **C / C++**
  - » **NULL pointer dereference**
  - » **Buffer overflow**
  - » **Memory leaks**
  - » **Un-validated user input**
  - » **Un-initialized data**
  - » **…….**
  - » **Style & Standards**
- **Java**
  - » **Concurrency**
  - » **Resource Leaks**
  - » **Web application vulnerabilities**
  - » **…….**
  - » **Style & Standards**

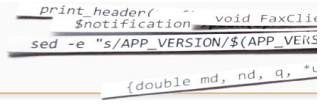
Klocwork

Source Code Security Initiatives

- NIST, **National Institute of Science and Technology**, part of **Department of Commerce**
  - » **Software Assurance Metrics and Tools Evaluation (SAMATE)**
  - » SAMATE Reference Dataset contains code snippets containing vulnerabilities/weaknesses in C/C++ and Java
- **Department of Homeland Security** (DHS) is also driving a security initiative called the **Common Weakness Enumeration** (CWE)
  - » CWE is developing a catalog of known software weaknesses collated from academic and industry sources
- OWASP Top 10
- PCI compliance

Klocwork

OWASP Top 10 2007

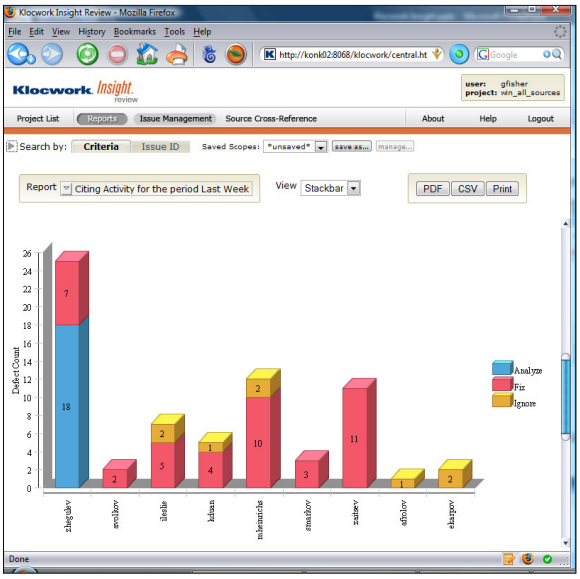


- Cross Site Scripting (XSS)
- Injection Flaws
- Malicious File Execution
- Insecure Direct Object Reference
- Cross Site Request Forgery (CSRF)
- Information Leakage and Improper Error Handling
- Broken Authentication and Session Management
- Insecure Cryptographic Storage
- Insecure Communications
- Failure to Restrict URL Access
- PCI compliance = OWASP support

Klocwork

Metrics & Trending

- Quality reporting at all levels, up to the minute, from system and desktop analysis
  - » Aggregate
  - » Drill down
  - » Scope
- Understand source code quality metrics by component, team or geography
- Build over build source code quality trending
- Source code analysis ROI information

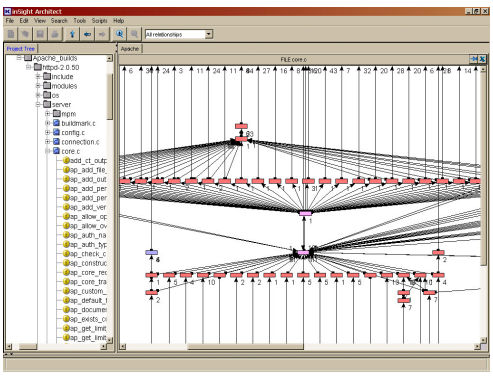


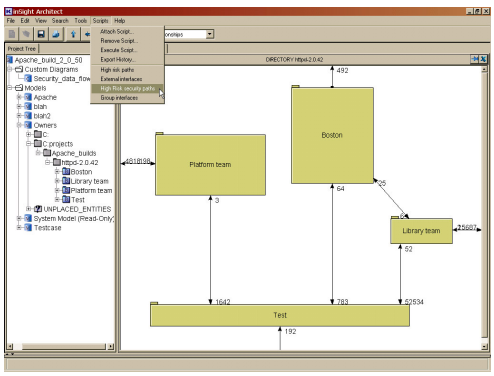
Klocwork

Architectural Analysis

Understand and Optimize your Architecture

- Graphical view of all components at all levels plus all relationships between components
- Reduce complexity, simplify architecture, improve maintainability / testability
- Create more re-usable, independent, longer lasting components
- Clean-up header file anomalies for shorter build times and improved maintainability
- Perform impact analysis and architectural improvement experimentation
- Create architecture rules and enforce secure design principles at a code level



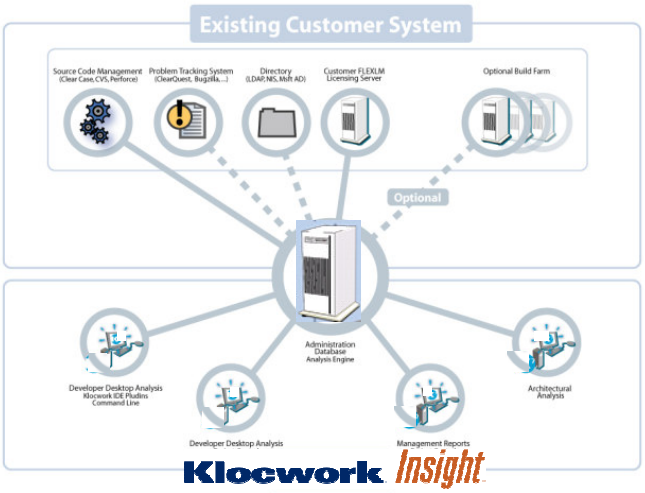


Klocwork

Environment Integration

Extending your existing enterprise investments

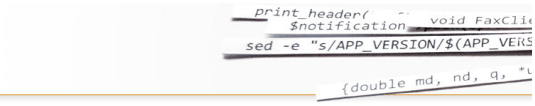
- Integrate with existing build process
  - » SCM system (ClearCase, Perforce, SVN, CVS, etc.)
  - » Build automation (make, ant, etc.)
  - » Build distribution
- Integrate with existing security environment
  - » Directory synchronization (LDAP, NIS)
- Integrate with problem tracking environment
  - » ClearQuest, Bugzilla, etc.



Motorola Case Study

- Six Sigma
- Corporate source code quality & security initiative
- Government & Public Safety
- Mobile Devices
- iDEN success story
- Connected Homes

Wrap-up



- Questions????????????
- I appreciate your time and interest
- Specific tool literature available
- Feel free to contact me at any time
  - » Tony.Czarnik@Klocwork.com
  - » 312.930.9828

Klocwork

Klocwork

IN THE UNITED STATES:
8 New England Executive Park
Suite 180
Burlington MA 01803

IN CANADA:
30 Edgewater Street
Suite 114
Ottawa ON K2L 1V8

1-866-556-2967
1-866-KLOCWORK
www.klocwork.com