What We’ve Learned from SATE

Arthur “Code Curmudgeon” Hicken
Chief Evangelist
Improvements since SATE IV

- More security rules
- Better handling of large code bases
- Better multi-core performance
- Smaller memory use
- Faster
Using Juliet as a standard

How do you compare tools?

Baseline for accuracy and performance

Repeatable results

No need to justify
## Juliet wish-list

<table>
<thead>
<tr>
<th>Easier Suite Analysis</th>
<th>More code</th>
<th>Publish unfound</th>
</tr>
</thead>
<tbody>
<tr>
<td>Better dead-code method</td>
<td>Improve code vs “other” issues</td>
<td>.NET</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Android</td>
</tr>
<tr>
<td></td>
<td></td>
<td>universally unfound</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Unexpected unfound</td>
</tr>
</tbody>
</table>
CWE wish-list

CWE status

• Too broad
• Ambiguous

CWE to map tools

• Ballpark – maybe
• Precise – no
• Two “rules” for the same CWE may look for entirely different things
• Two engines look in different ways, find different instances
Always:

- More rules
- More accurate
- Lighter/faster

Full CWE map

Possible new CWE items

Analytics
Current problems with Static Analysis

- False Positives – Perception vs. reality
  - It’s not just semantic
- False negatives
- Compare/combine tool results
- Finding what’s most important
- Coverage – what was really checked?
Pleasant discovery

- CWSS
- Scoring to understand what to work on
- Enable a risk-based approach
PIE on Pi – a proposed solution

Parasoft’s Process Intelligence Engine
Parasoft Development Testing Platform

Source Control

Execution/CI Build
- xTest 10.x (Server)
- xTest 9.x (Desktop)
- PHPMD
- FindBugs
- CheckStyle
- Other 3rd Party ...

Raw Observations

Policy Check

Intelligence (Dashboards/Reports)

Workflow (Task)

Practice/Domain Data (REST API)

Prioritized Findings

Web UI

Desktop IDE

External System

Requirements / Defects

Web UI

DTP

Process Intelligence Engine
Data from everywhere

Parasoft DTP

IDE

Static Analysis

Unit test

Peer review

Functional Test

Penetration Test

Build automation

Requirements

Bug tracking
What is P.I.E.

- Data from everything
- Open APIs

- Connectors
- Additional Data

- Reports
- Big data

- Events
- Triggers
- Timers
- Tasks

Open

Marketplace

Actions

Analytics
- Microsoft apps without programming
- Test alerts via iOS
- CWSS via Android
- NVD - Protecode
Samples outside the server

iOS Simulator – iPhone Retina (3.5-inch) / i Device

Projects   ProServeTools

Static Analysis Violations: 632
Unit Test Failures: 43

Warn Team!
- **Web**
  - [http://www.parasoft.com/jsp/resources](http://www.parasoft.com/jsp/resources)

- **Blog**
  - [http://alm.parasoft.com](http://alm.parasoft.com)

- **Social**
  - **Twitter:** @Parasoft @CodeCurmudgeon
  - **LinkedIn:** [http://www.linkedin.com/company/parasoft](http://www.linkedin.com/company/parasoft)
  - **Google+**:
    - +Parasoft +ArthurHickenCodeCurmudgeon
    - Google+ Community: Static Analysis for Fun and Profit