Static Program Analysis of JavaScript
Cryptographic libraries

Gopinath P
CDAC, Bangalore
Good Cryptographic libraries

Too many cryptographic libraries available, which one to choose?
Increasing prominence of JavaScript

- Once a client-side scripting language has evolved into server-side code
- Object Oriented Design
- Prototyping language
- Most number of code submissions in famous code repositories
Software Issues

- **Coding Flaws**: 70%
- **Configuration Flaws**: 8%
- **Design Flaws**: 5%
- **Process Flaws**: 8%
- **Requirement Flaws**: 9%

Source: Root Cause Analysis
http://csharpdeveloper.wordpress.com/2012/02/05/use-root-cause-analysis-to-get-to-defect-prevention-in-your-software-development-process
Coding practices

Do you do code reviews?

Source: Developer Productivity Report
Coding practices

Do you monitor and fix code quality problems?

- 39% Monitor, but do not fix
- 41% Fix some
- 12% Fix all
- 8% Do not monitor code quality

Source: Developer Productivity Report
Static Program Analysis

Source Code ➔ Model Extraction ➔ Intermediate Representations (IR) ➔ Analysis ➔ Results

Names Database/Symbol Table

<table>
<thead>
<tr>
<th>Name</th>
<th>Kind</th>
<th>Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>copy_item</td>
<td>function</td>
<td>item.c:25</td>
</tr>
<tr>
<td>item_cache</td>
<td>variable</td>
<td>item.c:10</td>
</tr>
<tr>
<td>color</td>
<td>parameter</td>
<td>palette.c:23</td>
</tr>
<tr>
<td>header.h</td>
<td>file</td>
<td>shapes.c</td>
</tr>
</tbody>
</table>

Abstract Syntax Tree (AST)

Control Flow Graph (CFG)

Call Graph
Plato

- A JavaScript Static Analysis Report Generator
- Executes itself on a Node.js engine
- Installation:
  - npm install -g plato
Plato

- The interactive report comprises of:
  - Maintainability score
  - Lines of code
  - Estimated Error Count
  - Linter Error Count (JSHint and ESLint)

- To run the tool: `plato -r -d <output-dir> <input-dir>`

- Demo...
Thank you!