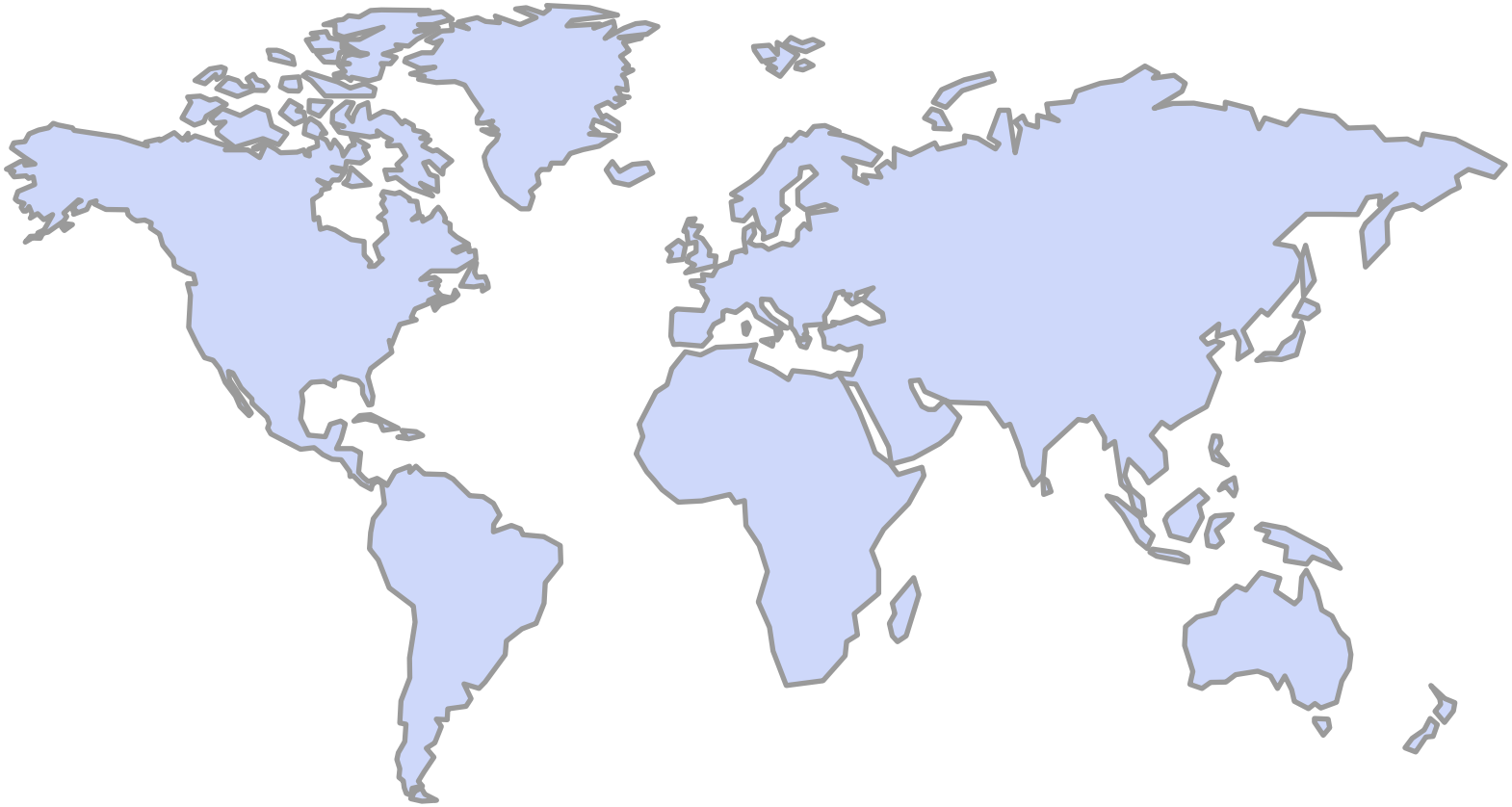
Application Security Tools in 2012

We already live in the future.

Eric Heitzman

- WW Tech Specialist, Rational Security Tools



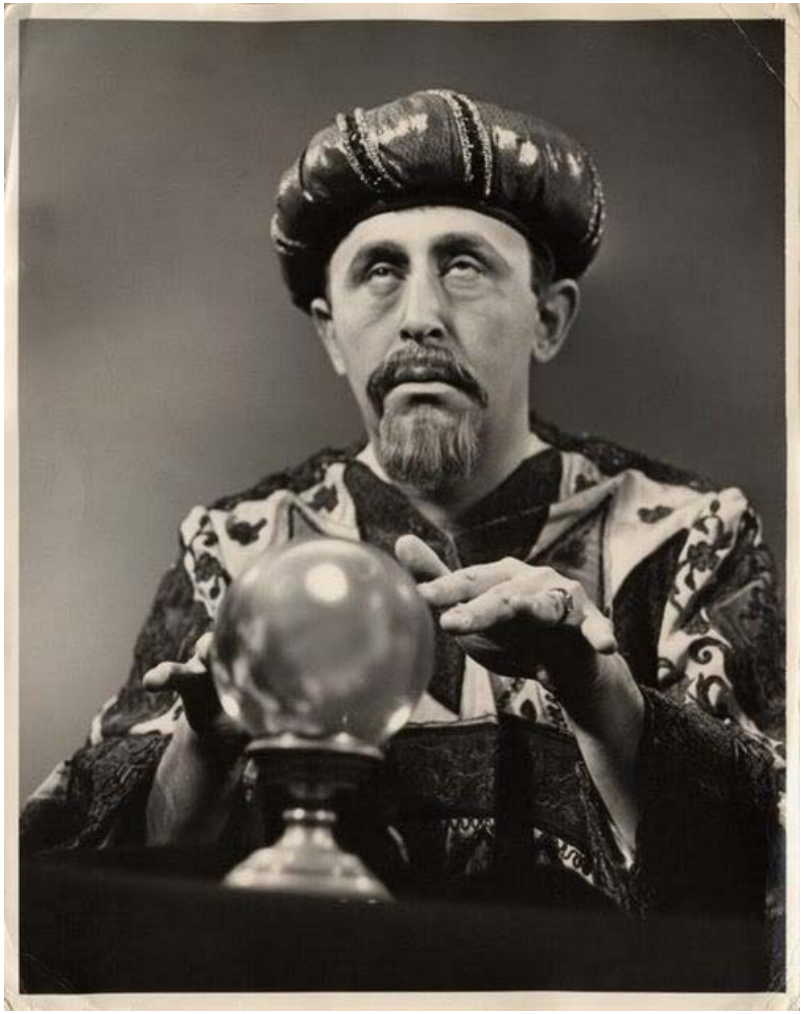
Foundstone » McAfee » MANDIANT™

OUNCE LABS » IBM

Where are we headed?

Crystal Ball

- What will be discussed in 2012 regarding application security tools?



Big Apps are getting Bigger

- 3-tier architecture is gone
- Frameworks do more than ever
- Apps leverage external components
- Portal apps connect many systems
- Java and .NET are leading the charge

Small Apps are Proliferating

- Cars: “Average16MLoC, 6 antennas, ring bus topology”


»


- Power: Generation, distribution, metering


?

- Mobile: iOS, Android, Win Mobile 7, BlackBerry, etc.

iOS

Windows Mobile


?

- There are more apps, doing more critical things, more connected to each other.

Industry demands 2012

Broader Platform Support

- Adding support for new languages

Advanced Framework Support

- Framework for a Framework

Industry demands 2012

End to End Analysis

- Modular Analysis

Lightweight Analysis

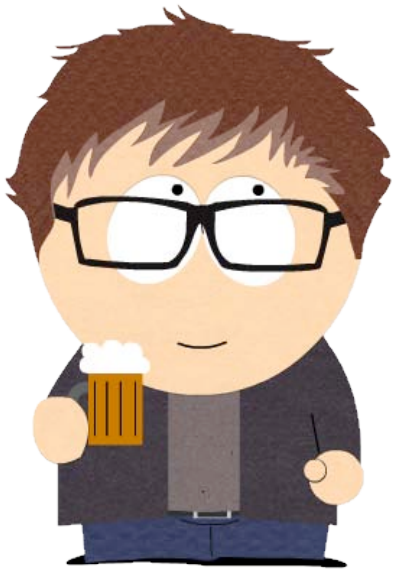
- String Analysis
- Incremental Analysis

Contact

Eric Heitzman

WW Technical Specialist, Application Security Tools

- eric.heitzman@us.ibm.com
- 805.540.0306



Definitions for terms used in this presentation

Framework for a Framework

- A meta-framework for describing how frameworks affect data flow, control flow, data validation, web service definitions, and so on.

Modular Analysis

- The tool learns as it scans.
- Each scan adds “rules”, so when that component is included by another project
  - Analyze faster
  - Analyze even when the original code is not available

Definitions for terms used in this presentation

String Analysis

- Automatically identify validation routines, determine what vulnerability categories are mitigated by each routine.

Vulnerability Analysis Cache

- For repeat scans of the same code base, saving one of the main object models increases scan speeds by ~8x

Incremental Analysis

- Improvement on “Vulnerability Analysis Cache”, allows the model to be selectively rebuilt based on only those files which have changed.