MILCOM 2015
LEVERAGING TECHNOLOGY—THE JOINT IMPERATIVE
OCTOBER 26–28, 2015 · TAMPA, FL

Tutorial: Practical Program Analysis for Discovering Android Malware

Module 5: **Continuing Beyond the Tutorial**

Suresh Kothari – kothari@iastate.edu
Benjamin Holland – bholland@iastate.edu

Acknowledgment: co-workers and students
DARPA contracts FA8750- 12-2-0126 & FA8750-15-2-0080

ensoft
conquer complexity

IOWA STATE UNIVERSITY

Agenda

- Future Work
- Resources for Going Further
- Feedback

DARPA STAC Project

- **Space/Time Analysis for Cybersecurity (STAC)**: Detect algorithmic complexity (AC) and side channel (SC) vulnerabilities by analyzing variations in space-time complexities along different execution paths
- **Requirement**: Analyze Java byte code taking into account the library calls
- **Performance Goal**: Scalable and accurate detection of AC and SC vulnerabilities

Ongoing Work

- Continue to improve program graphs to account for sensitivities
  - Context Sensitivity
  - Object Sensitivity
  - Type Sensitivity
  - Flow Sensitivity

Atlas gives you the raw information you need to deal with any of these problems in a manner of your choosing.

Agenda

- Future Work
- Resources for Going Further
- Feedback

Resources for Going Further

- Atlas for C/C++, Java, Jimple (bytecode)
- More Atlas Tutorials
  - http://ensoftatlas.com/wiki/Learning_Atlas
- Additional Atlas Projects
  - https://github.com/EnSoftCorp
- EnSoft Support
  - support@ensoftcorp.com

Agenda

- Future Work
- Resources for Going Further
- Feedback

Please help us improve!

- Quick survey to help us improve this content
  - Short Link: https://goo.gl/8GEj35

- Please email us any other comments, questions, etc.
  - Suresh Kothari: kothari@iastate.edu
  - Ben Holland: bholland@iastate.edu

Thank you!