SATE V – Red Lizard Software

Dr Franck Cassez

Red Lizard Software/NICTA

SATE V workshop, March 14th, 2014, Gaithersburg, MD, USA

http://www.redlizards.com

Australian Government

Department of Broadband, Communications and the Digital Economy

Australian Research Council

NICTA Funding and Supporting Members and Partners

Australian National University

UNSW THE UNIVERSITY OF NEW SOUTH WALES

NSW GOVERNMENT Trade & Investment

ACT GOVERNMENT

State Government Victoria

THE UNIVERSITY OF MELBOURNE

THE UNIVERSITY OF SYDNEY

Queensland Government

Griffith UNIVERSITY

QUT Queensland University of Technology

THE UNIVERSITY OF QUEENSLAND AUSTRALIA

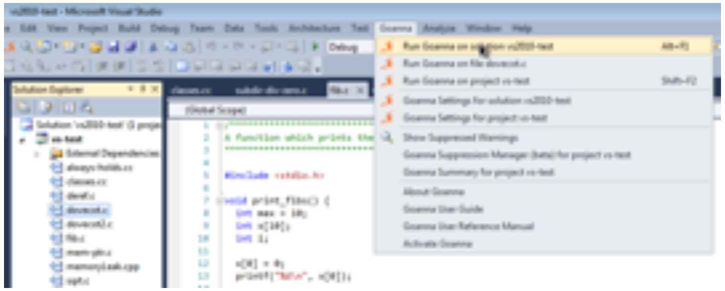
Red Lizard Software

Red Lizard Software
Funded 2009
Engineering Staff: 7

Approx 600 researchers
Software Systems Research Group

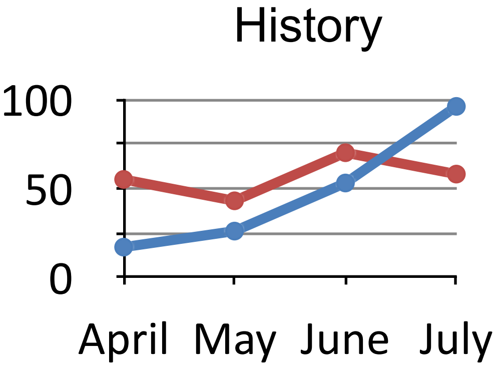
Goanna Static Analysis Tool

C/C++ projects


vs2010-test - Microsoft Visual Studio
Edit
View
Project
Build
Debug
Team
Data
Tools
Architecture
Test
Goanna
Analyze
Window
Help
Debug
Run Goanna on solution vs2010-test Alt+F1
Run Goanna on file dovecot.c
Run Goanna on project vs-test Shift+F2
Goanna Settings for solution vs2010-test
Goanna Settings for project vs-test
Show Suppressed Warnings
Goanna Suppression Manager (beta) for project vs-test
Goanna Summary for project vs-test
About Goanna
Goanna User Guide
Goanna User Reference Manual
Activate Goanna
Solution Explorer
Solution 'vs2010-test' (3 projects
vs-test
External Dependencies
always-holds.cc
classes.cc
deref.c
dovecot.c
dovecot2.c
fib.c
mem-ptr.c
memoryLeak.cpp
opt.c
classes.cc
subdir dir zero.c
fib.c
(Global Scope)

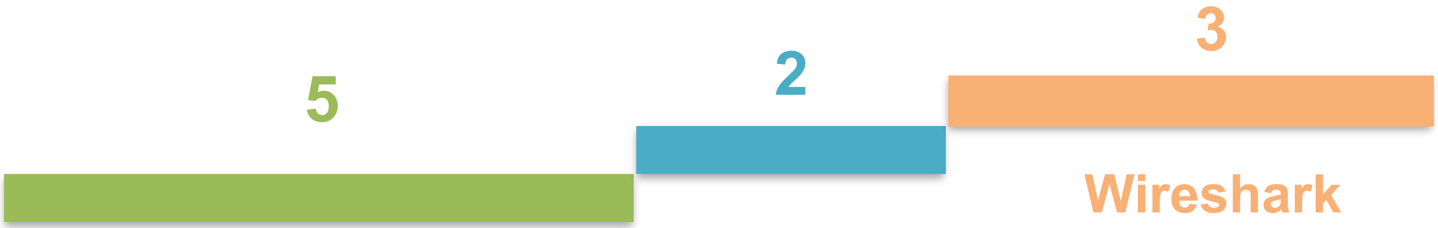
```
/*************************************
 A function which prints the
*************************************

#include <stdio.h>

void print_fibs() {
  int max = 10;
  int x[10];
  int i;

  x[0] = 0;
  printf("%d\n", x[0]);
```

Static Analysis + Model-Checking



- Fully automatic
- Whole program analysis
- Intra-procedural context sensitive
- Inter-procedural bottom-up
- Pointer aliasing
- Refinement

Resources for SATE V



5

Synthetics

2

Automating
XML formatting
Set up VM

3

Wireshark
Asterisk
Review
Final Report

10 days

3 Staff: 2 Engineering Staff, 1 researcher

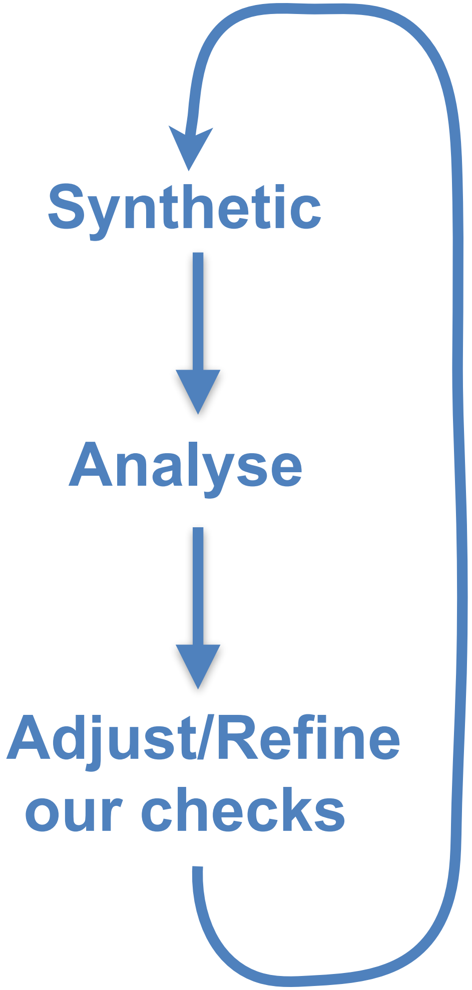
Hardware: Intel i7, 3Ghz, 8GB, Linux

Analysis Plan

1 – Map CWE to Goanna checks

2 – Source of FP and FN

3 – Adjust/Modify/Add check



Synthetic

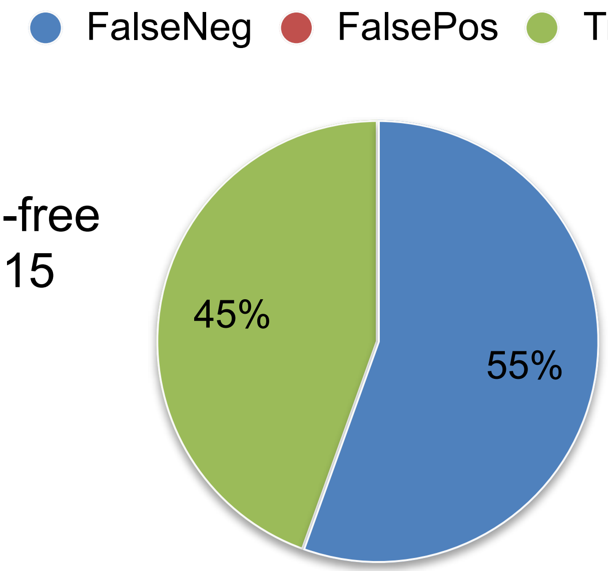
Analyse

Adjust/Refine our checks

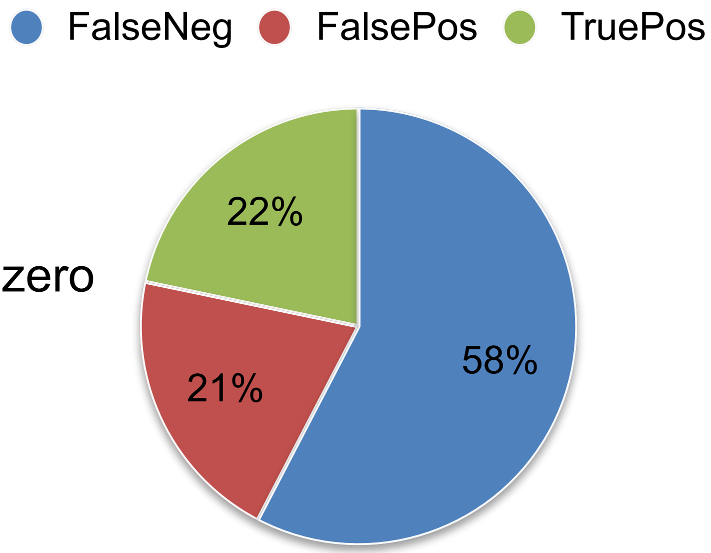
Total: 3 iterations

Results Juliet Test Suite

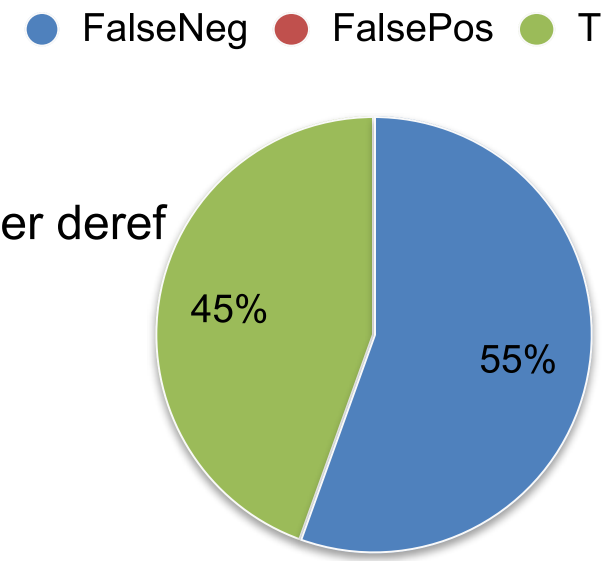
Double-free
CWE 415



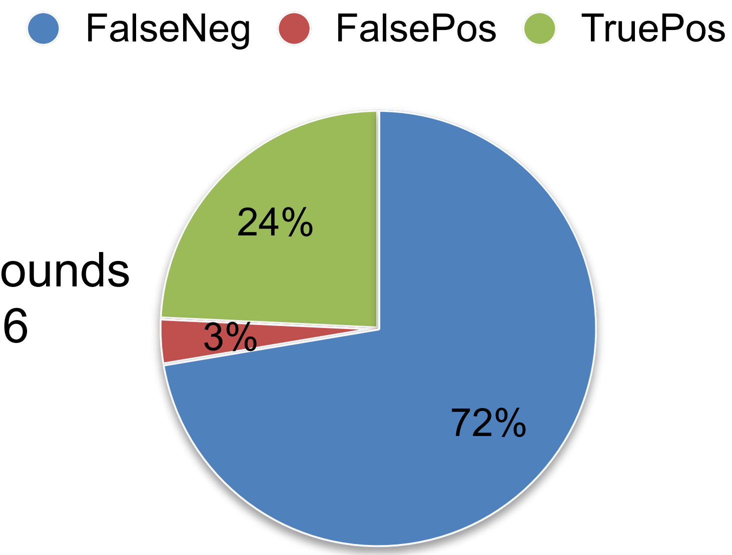
Divide-by-zero
CWE 369



NULL-pointer deref
CWE 476

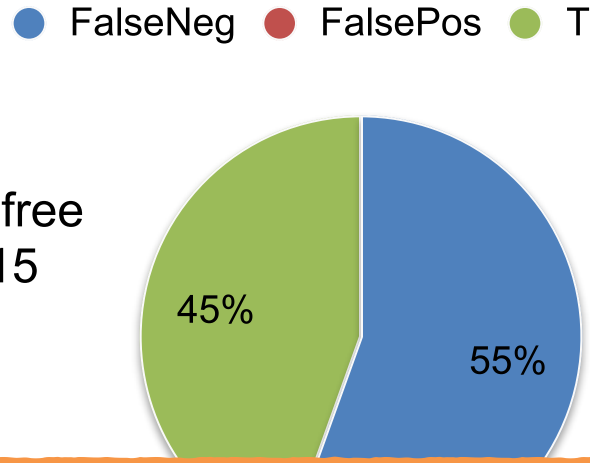


Array-out-of-bounds
CWE 124, 126

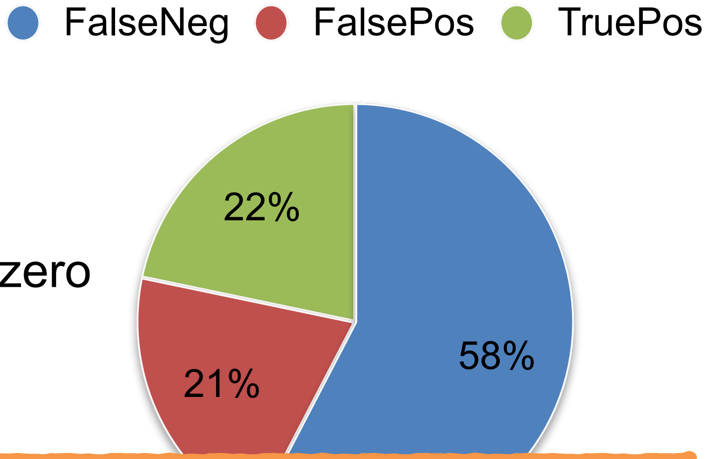


Results Juliet Test Suite

Double-free
CWE 415



Divide-by-zero
CWE 369



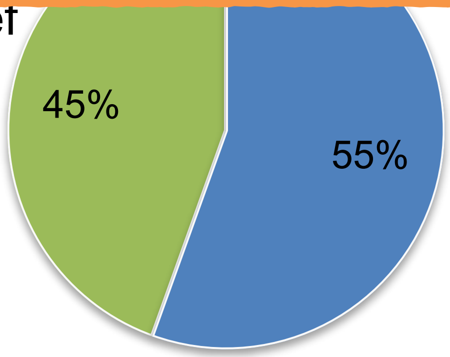
FalseNeg. *Due to custom “malloc”, syntactic variations of Goanna checkers.*

FalsePos. *Goanna checker is more versatile than CWE: checker for all methods, but CWE for “static” methods.*

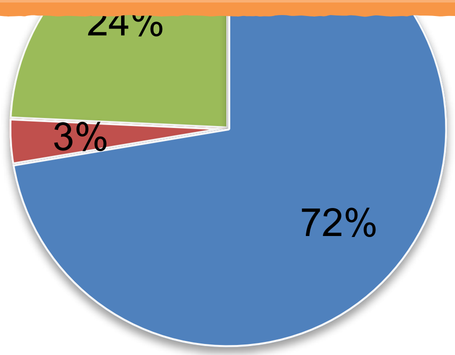
Solution*: refine Goanna checkers, customization of some checkers*

s

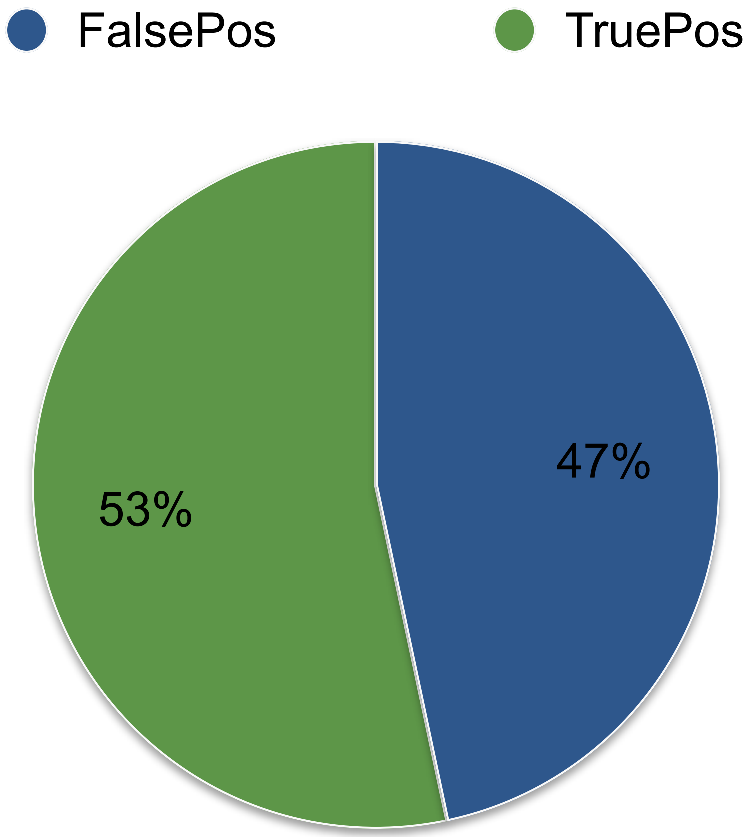
NULL-pointer deref
CWE 476



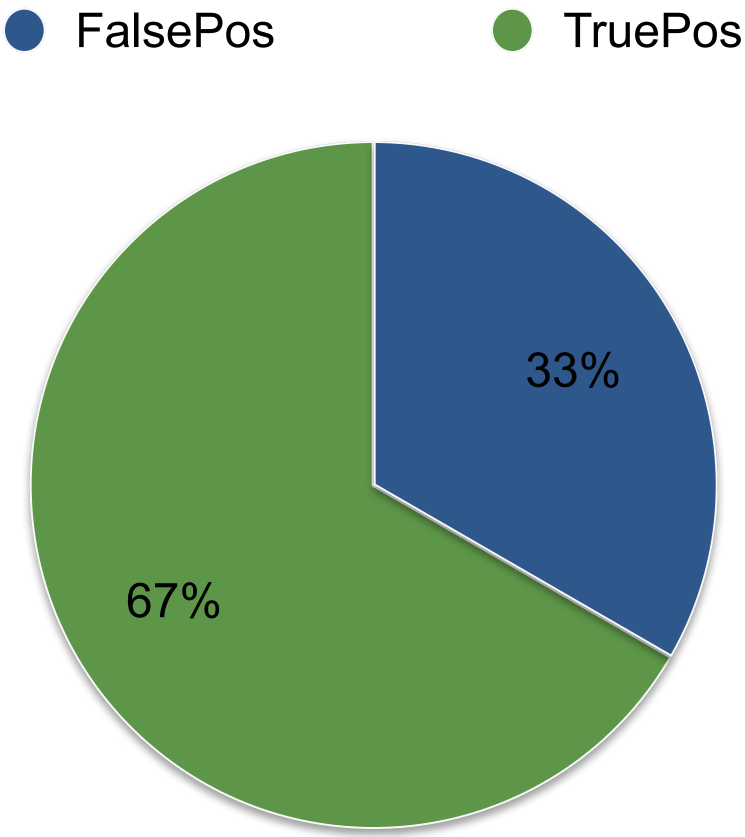
Array-out-of-bounds
CWE 124, 126



Results Wireshark/Asterisk



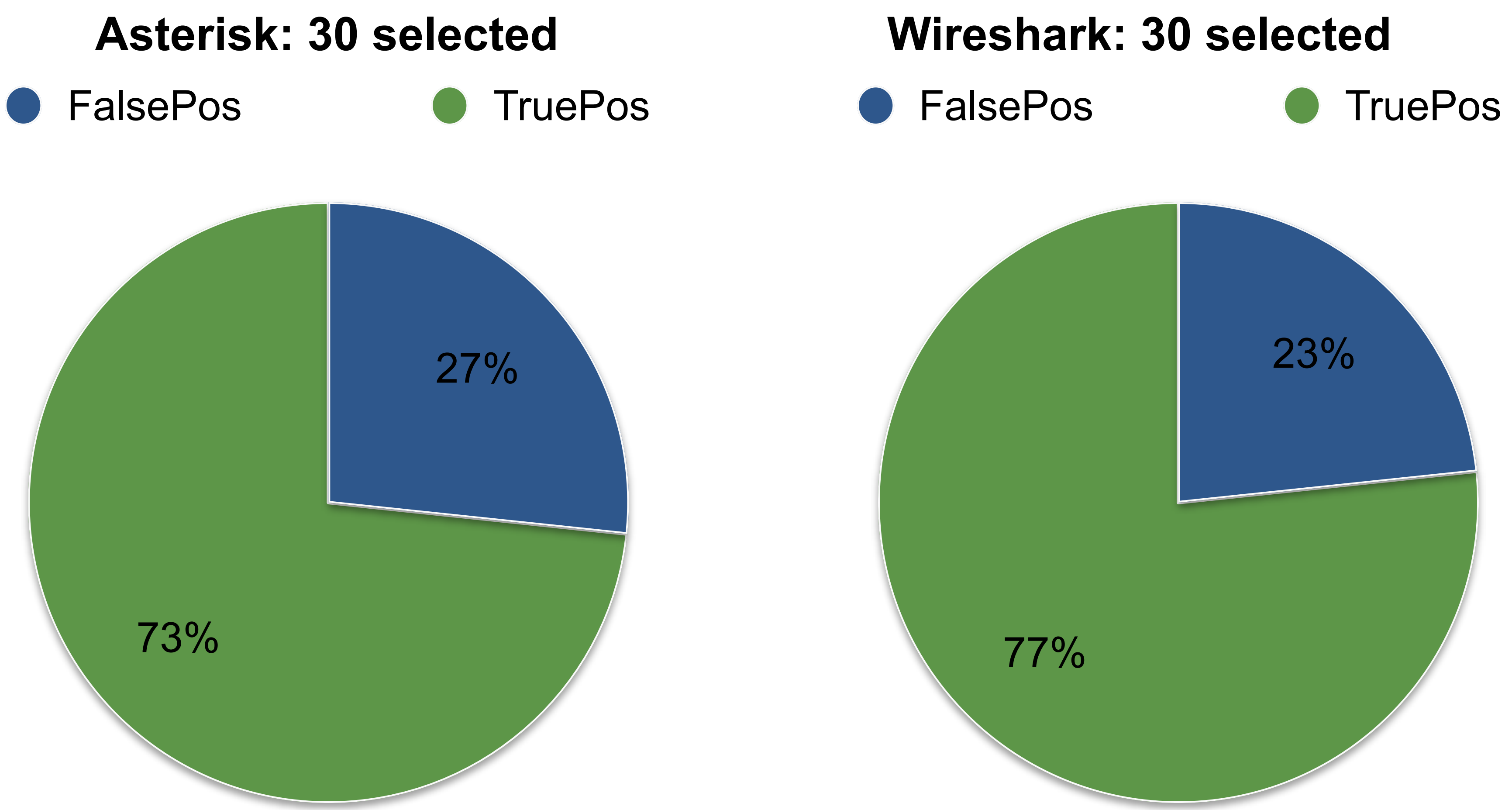
Asterisk: 30 selected



Wireshark: 30 selected

NIST results

Results Wireshark/Asterisk



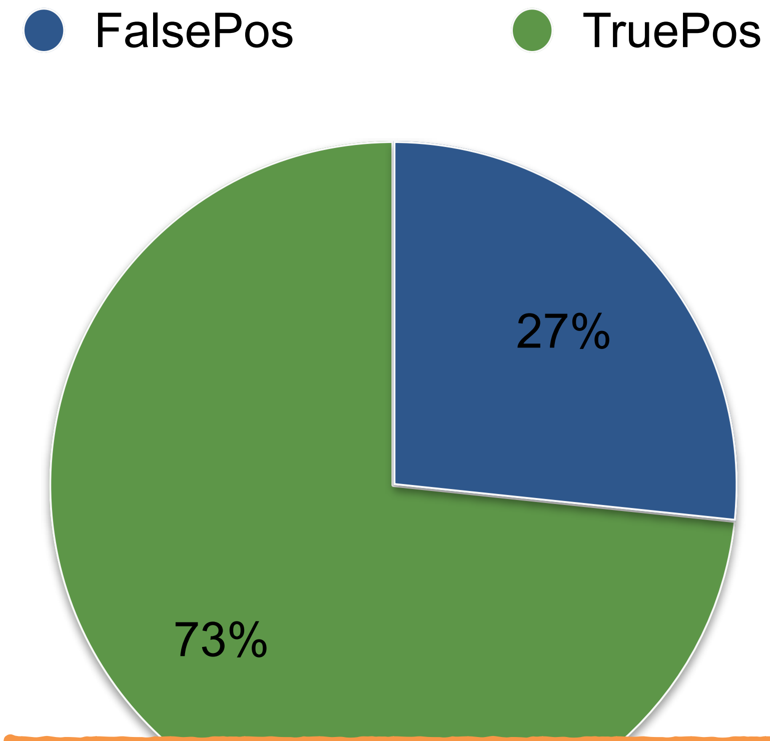
Asterisk: 30 selected

Wireshark: 30 selected

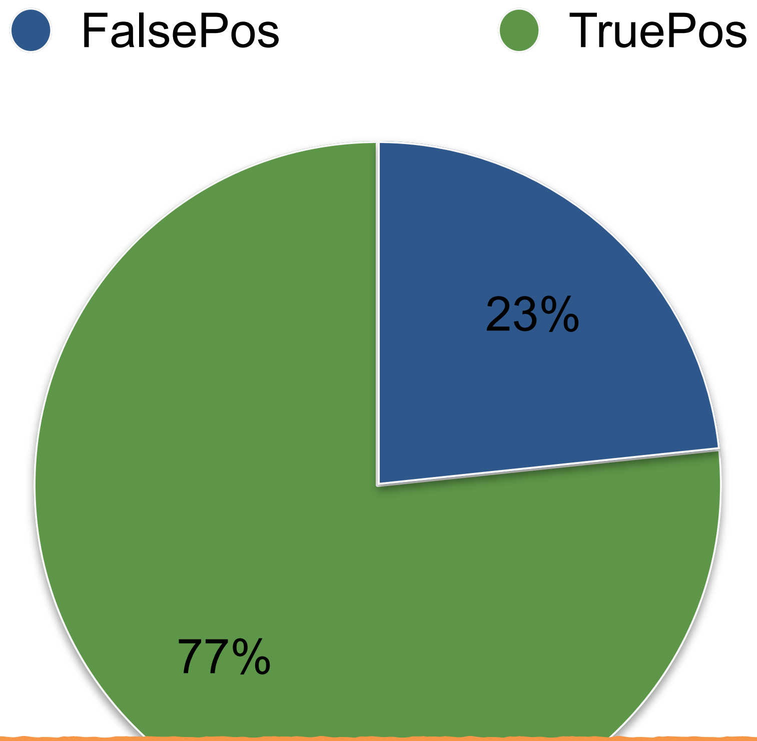
Our Evaluation

Results Wireshark/Asterisk

Asterisk: 30 selected



Wireshark: 30 selected



Example of disagreement:
NIST evaluator: FalsePos. *"yes a file is read […] but this is a config file so harmless."*

RedLizards: TruePos. *The information that the file is a config file is not available for the software analyser Goanna and thus this file cannot be trusted.*

Lessons Learnt

- New checks and map CWE to Goanna checks
- Classes of defects we are not looking for
  - Syntactic
  - Variations of Goanna checks (some are now implemented)
  - Challenging defects (require inter-procedural, alias analysis, etc)
- Juliet test cases
  - Added to our nightlies tests
  - Used in the next generation Goanna

That’s a (Australian) Goanna!