STA: Security Type System for Android (Chapter 8, CSF'18)

Sound Permission-dependent Type

Integration with Decidable Type Inference

STA Based Implementation Prototype

Verification:

Securing
High Level
System
Designing

FOT: Fuzzing Orchestration Framework (Chapter 5, ESEC/FSE'18)

Versatile in Integrated Functionality

Configurable Fuzzing Strategies

Extensible Programming Interfaces

Directedness Extension

Hawkeye: Directed Grey-box Fuzzing (Chapter 6, CCS'18)

Robust Directedness Mechanism

Integration with Static Analysis

Seed Prioritization and Schedule

Adaptive Strategies Across States

Multithreading Extension

Doublade: Thread-aware Grey-box Fuzzing (Chapter 7, submitted)

Thread-Interleaving Feedback

Awareness of Threading Context

Diversity Guarantee Across Executions

Testing:
Detecting
Low Level
Implementation
Vulnerabilities