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

Sound Permission-dependent Security Type System

Integration with Decidable Type Inference

Security Type System Based Implementation Prototype

Verification: Securing High Level System Designing

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

Versatile in Integrated Fuzzing Functionality

Configurable Fuzzing Strategies across Procedures

Extensible Application Programming Interfaces
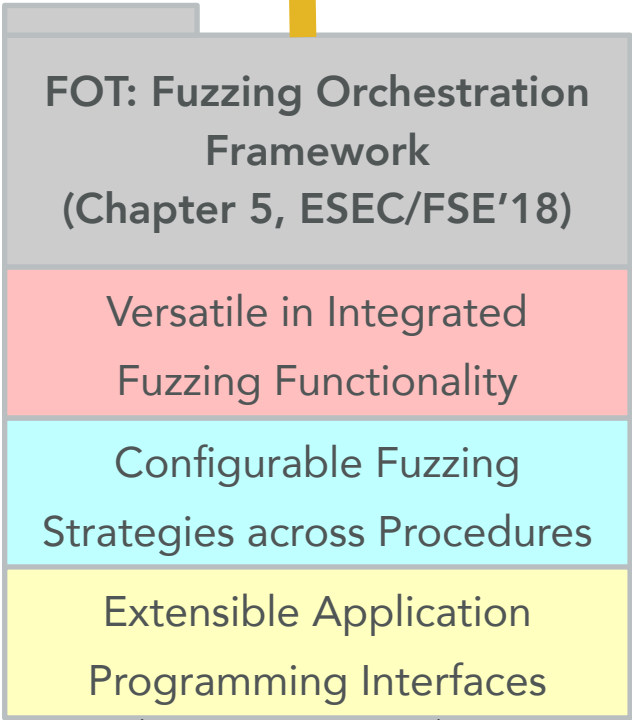
Testing: Detecting Low Level Implementation Vulnerabilities

Directedness Extension
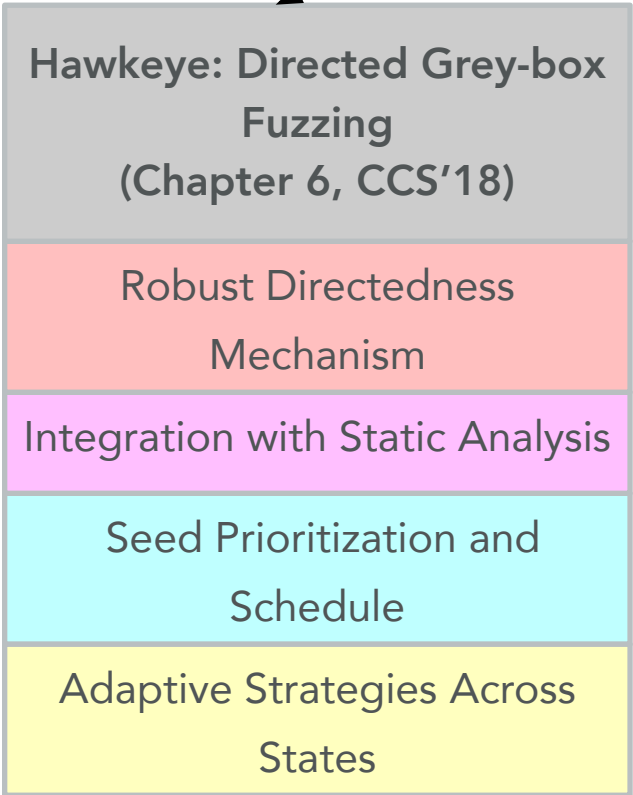
Multithreading Extension

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

Robust Directedness Mechanism

Integration with Static Analysis

Seed Prioritization and Schedule

Adaptive Strategies Across States

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

Thread-Interleaving Feedback

Awareness of Threading Context

Diversity Guarantee Across Executions