Cybersecurity Research Acceleration Workshop and Showcase

October 11, 2017 | Indianapolis, IN

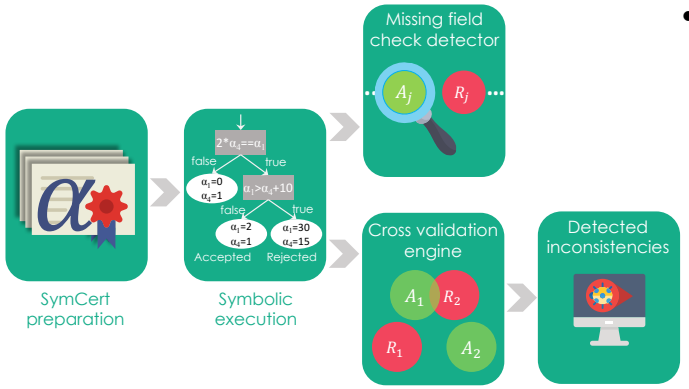
# Quad Chart for: A Principled Approach Aiding the Development of a Compliant Internet PKI

## Challenge:

- Complex structure of X.509 PKI certificate
- Cryptographic libraries
- Code/logic coverage:
- Standard specification

## Solution:

- Employing Symbolic Execution (SE)
- Mitigating path explosion in SE
  - Using specially crafted input
  - Bypassing crypto. functions
- Extracting the certificate input universe
- Partitioning the universe to:
  - Accepting universe
  - Rejecting universe
- Launching differential testing




## Value proposition:

- Fully leverage the open source nature of libraries
- Enabling users to find more in-depth bugs

## What we need to TTP

- Automated instrumentation
- Analysis engines
- Your input

**NSF CRII SaTC #1657124**
**The University of Iowa**
PI: Omar Haider Chowdhury,
Assistant Professor of Computer Science

## Contact

- omar-chowdhury@uiowa.edu