Center for Embedded Systems

An NSF Industry/University Cooperative Research Center

Verifiable Firmware Update Mechanisms for Embedded Systems

Ning Weng, SIUC

Spyros Tragoudas, Joseph Lenox, Veeresh Dandur

SIU Southern Illinois University CARBONDALE

NATIONAL SCIENCE FOUNDATION

ASU Ira A. Fulton Schools of Engineering ARIZONA STATE UNIVERSITY

Project Overview and Description

- **Project Description**
  - Verify/Validate software running on remote untrusted ES
  - Empower ES to determine whether software updates are authorized

Project Overview and Description

- **Current mechanisms**
  - Public key infrastructure
  - Secure hardware extension
- **Challenges**
  - Embedded systems constraints: resource, connectivity
  - Operational issues: multiple independent root authorities, certification revocation,

Practical integrity solution for constrained ES w/existing mechanisms

Approach

- **Authority-based**
  - Software signature
    - Local verification
    - Whitelist
  - Public Key Infrastructure
    - ex: X.509
  - Challenge
    - Network connectivity

Approach

- **Host-assisted**
  - Rule/Anomaly-based
  - Rules are preloaded
  - Challenge
    - Securing host monitoring
  - Existing Hardware extension solution
      - Secure hardware extension (SHE) on Freescale MPC564xs

Project Tasks/ Deliverables

	Description	Date	Status
1	Review adversary attack methods and verification mechanism specification	10/13	
2	Authority-based solution	1/14	
3	Host-based solution, acquire candidate systems for platform evaluation	7/14	
4	Prepare final report	8/14	