Addressing 0-days in EDS

J. Peter Brady, Ira Ray Jenkins, Prashant Anantharaman, Sameed Ali, Andrew Truong, Sean Smith; *Illinois:* David Nicol, Kartik Palani, Elizabeth Reed.

ENERGY DELIVERY SYSTEMS ARE VULNERABLE

- Computer systems are rife **with security holes and 0-days**.
- Embedded systems and ICS can **be hard to patch**; 0-days become **forever days.**
- In EDS, consequences can be **dire**.

RESEARCH VISION

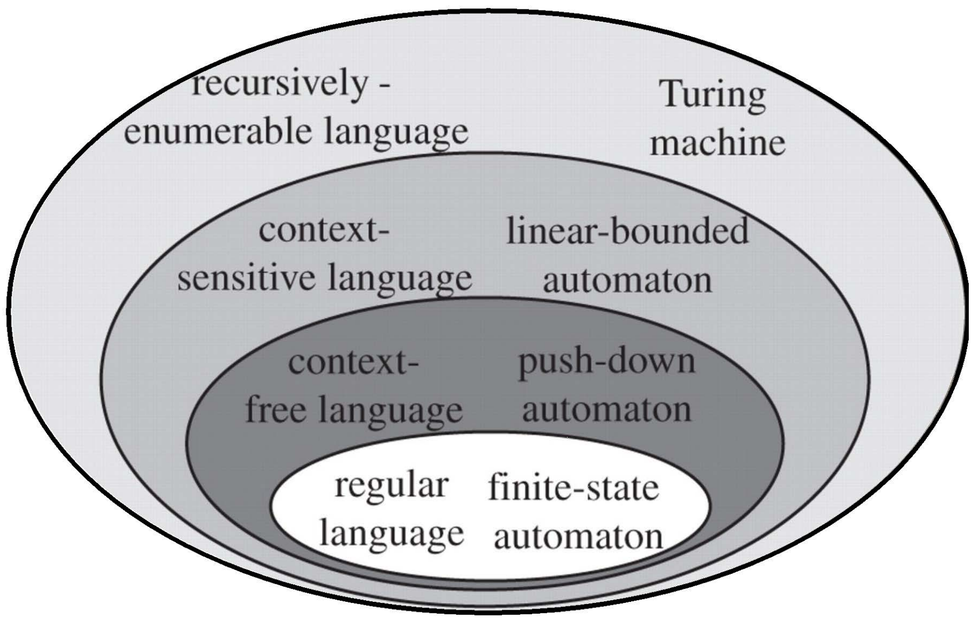
New tools based on new scientific foundations:

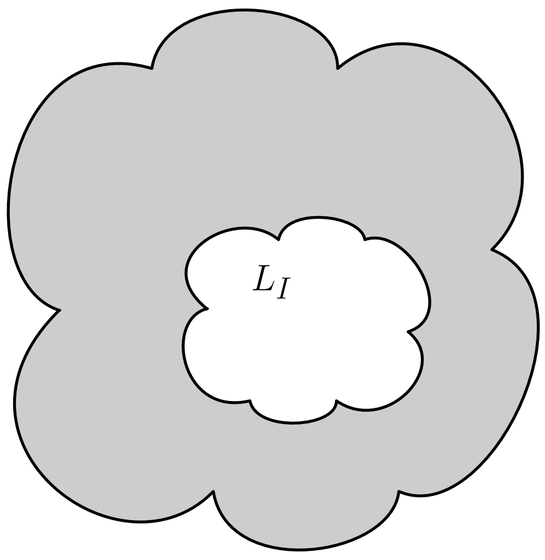
- **Prevention** of 0-days in the first place.
- **Mitigation** of damage from holes discovered after deployment.
- **Snap-in patching** preserving availability
- **Evaluation** of effectiveness of these tools when scaled up to long-lived EDI.

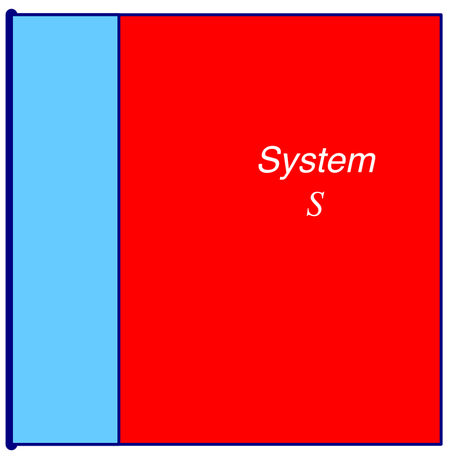
RESEARCH ROADMAP: PREVENTION

LangSec: Using formal language theory to:

- specify precisely the input language on an attack surface
- build high-assurance parsers that block crafted input attacks
- build fuzzing tools to test for holes in deployed systems





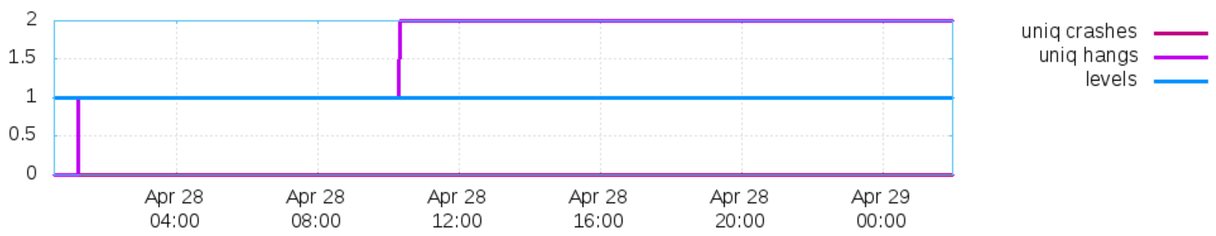


SOME RESULTS FROM OUR WORK

Hardened parsers available for:

- DNP3
- GOOSE
- MQTT
- ICCP
- C37.118
- Modbus

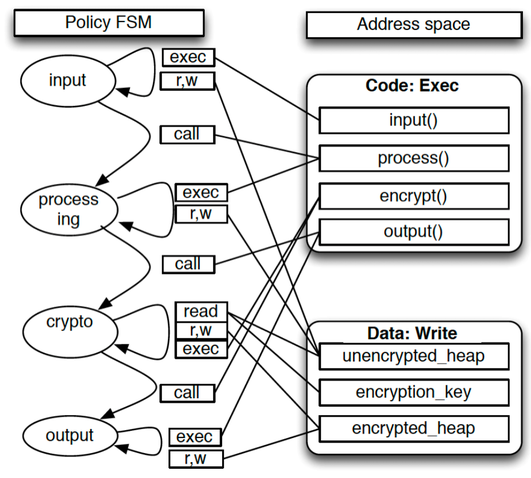
With others in progress.

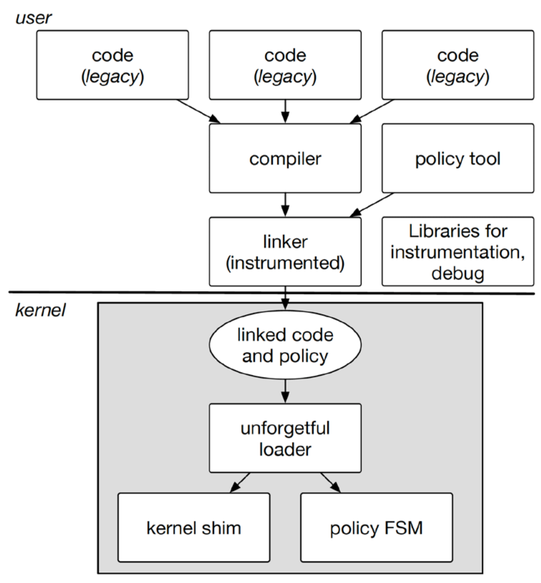


RESEARCH ROADMAP: MITIGATION

ELFbac: Custom linker/loader and Linux kernel to enforce intra-process memory isolation

- Compatible with current OS and build tools
- Compatible with legacy software





SOME RESULTS FROM OUR WORK

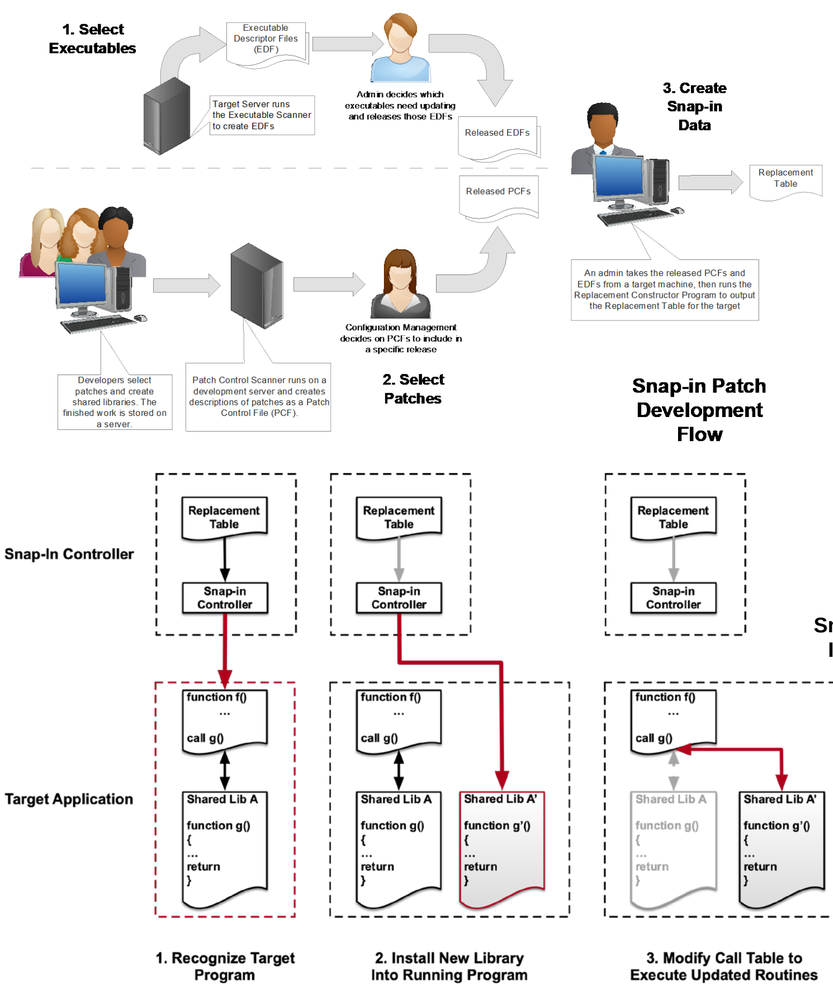
Proof of concept implementations:

- stopping OpenSSH Roaming vulnerability
- stopping Spectre V1

RESEARCH ROADMAP: SNAP-IN PATCHING

Novel approach to permit stakeholders to install ***patches without downtime***

- Stakeholders can still test patches
- Stakeholders can control when and how patches are applied



IMPACT ON STATE OF GRID SECURITY

- ***Preventing vulnerabilities*** in the first place
- ***Limiting damage*** from them
- Making ***patching them easier***

COLLABORATION OPPORTUNITIES

Cooperation, support, and guidance from industry partners in the following areas would benefit this research activity:

- EDS systems with protocols/interfaces at risk of adversarial exposure
- EDS systems whose internal compromise could threaten energy resilience
- EDS systems where continued availability is highly critical

Contact: jenkins@cs.dartmouth.edu, sws@cs.dartmouth.edu

Activity webpage: https://cred-c.org/researchactivity/ResilientScale

FUNDING SUPPORT PROVIDED BY THE U.S. DEPARTMENT OF ENERGY AND THE U.S. DEPARTMENT OF HOMELAND SECURITY