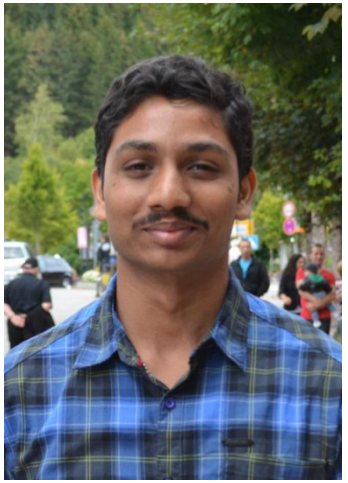
Distributed Just-Ahead-Of-Time Verification of Cyber-Physical Critical Infrastructures

Award #1446471


Saman Zonouz
(Rutgers)


Katherine Davis
(TAMU)


Pete Sauer
(UIUC)

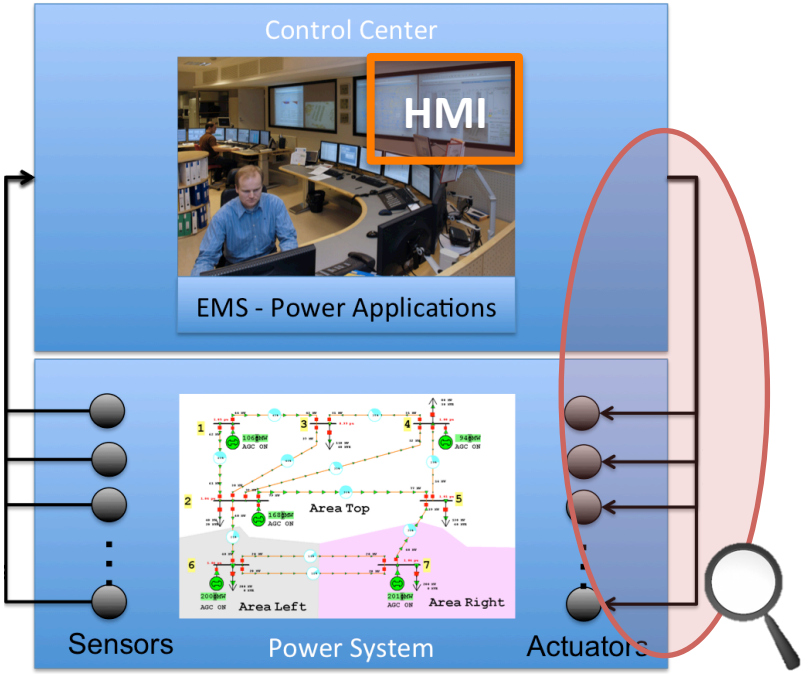

Sriharsha Etigowni
(Rutgers)

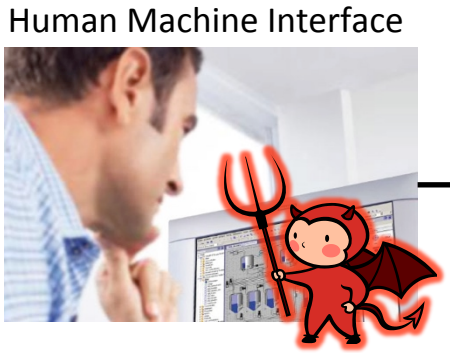

Bogdan Pinte
(TAMU)

Cyber-Physical Security

Real-World Threat

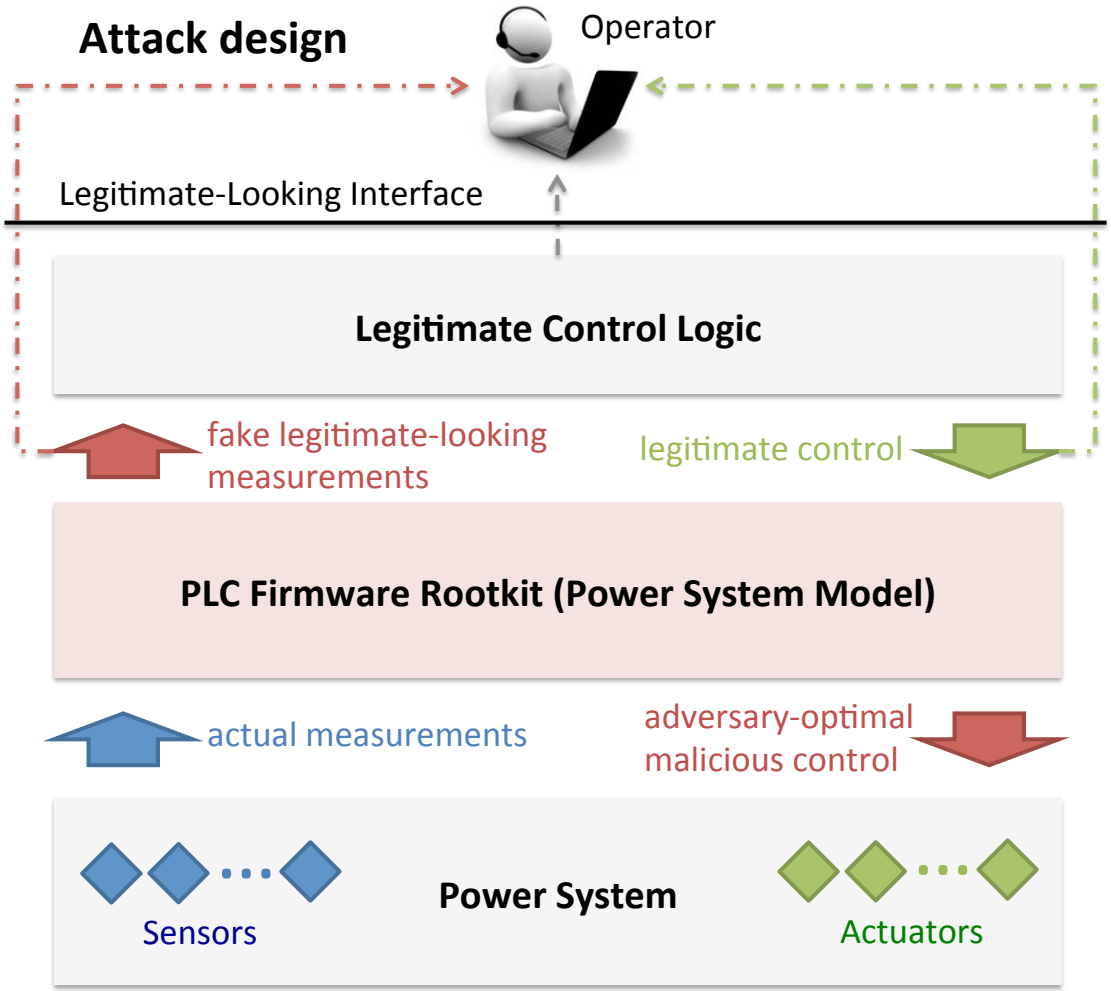
- Example: Stuxnet malware
  - *Compromises HMI server (4 zero-day exploits)*
  - *Intercepts the PLC code upload*
  - *Uploads malicious controller code on PLC instead*
  - *Replays a normal operational status on HMI screen*



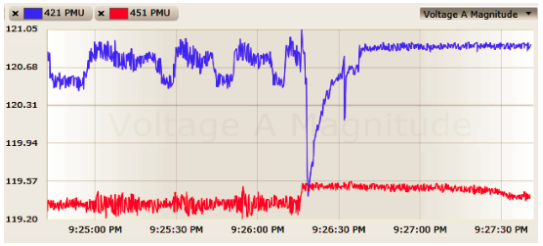


Malicious Controller

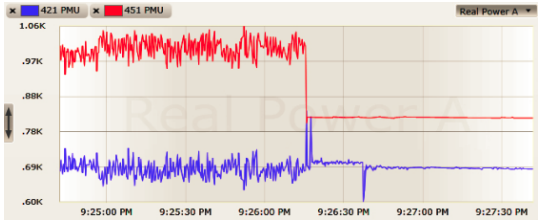
Controller Rootkit (NDSS'17)



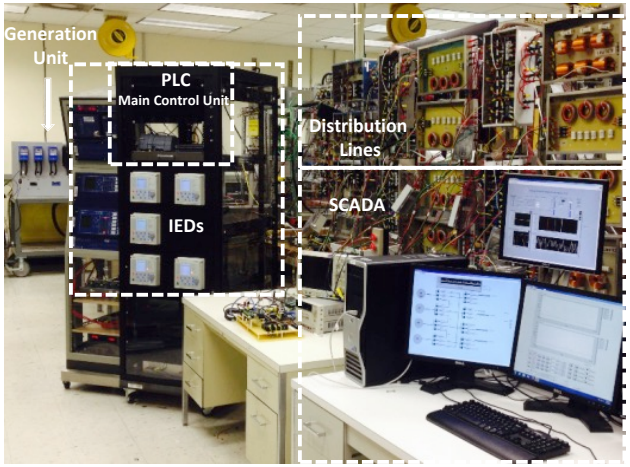
Real-world Attack Demo



(b) Voltage Magnitude



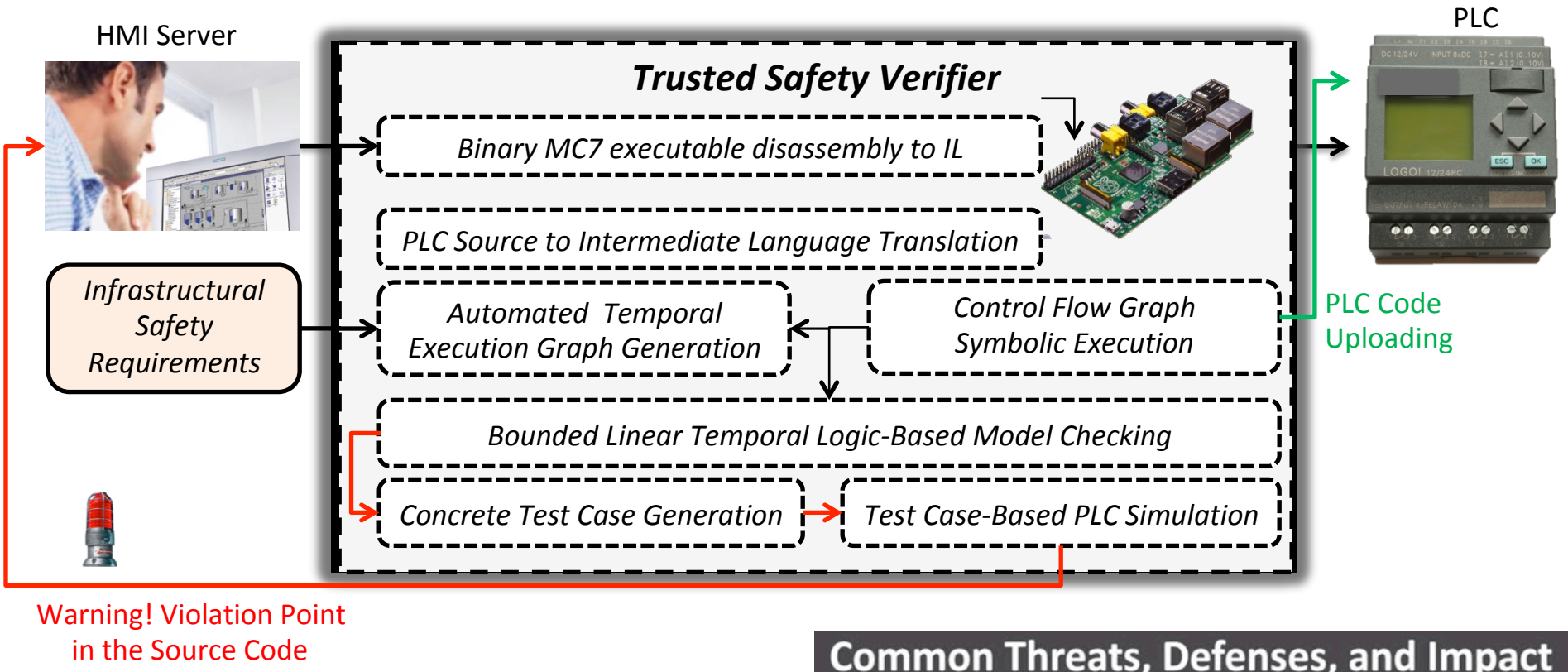
(d) Power



Maliciously functional firmware modification vs. **BlackEnergy3**'s firmware corruption.

Provide stealth in highly dynamic environments vs. **Stuxnet**'s sensor data record-and-replay.

Solution and Findings (CCS'17, NDSS'14)



- TechTransfer: with Siemens 2015-present
  - To integrate code verification in PLC code development IDE
- Education activity examples:
  - CreaTECH workshop for SWE 2017