Resilient, adaptable, and secure systems

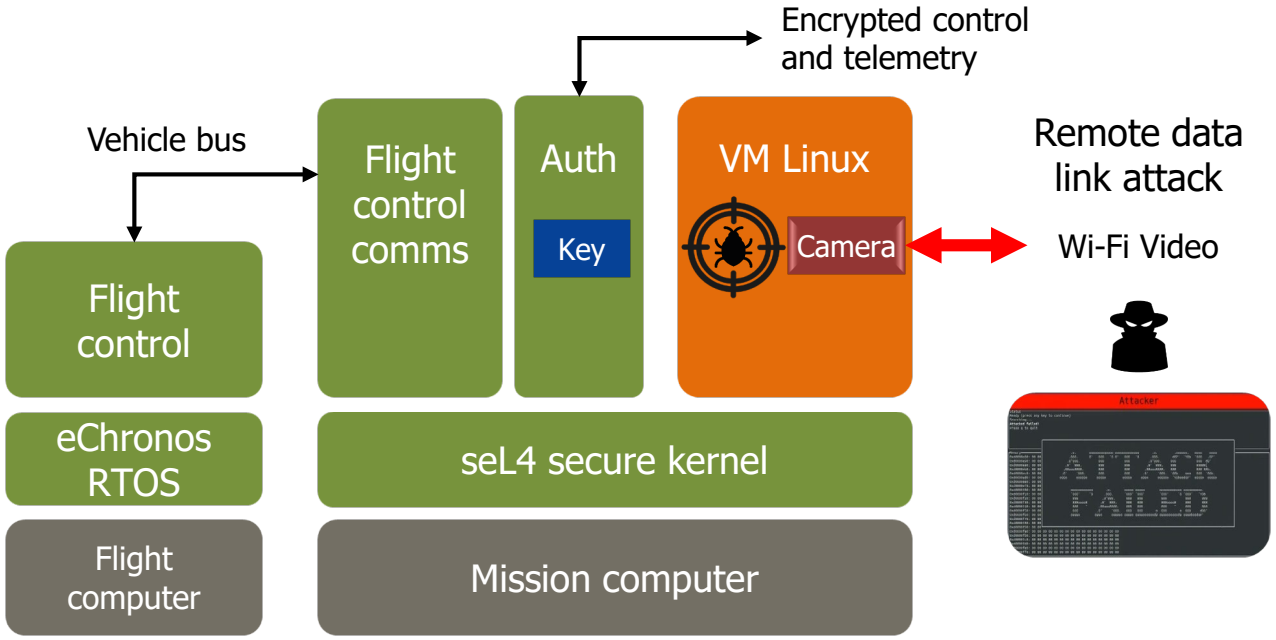
Kathleen Fisher
Director, Information Innovation Office (I2O)

November 2022

Formal methods can work

High Assurance Cyber Military Systems (HACMS)

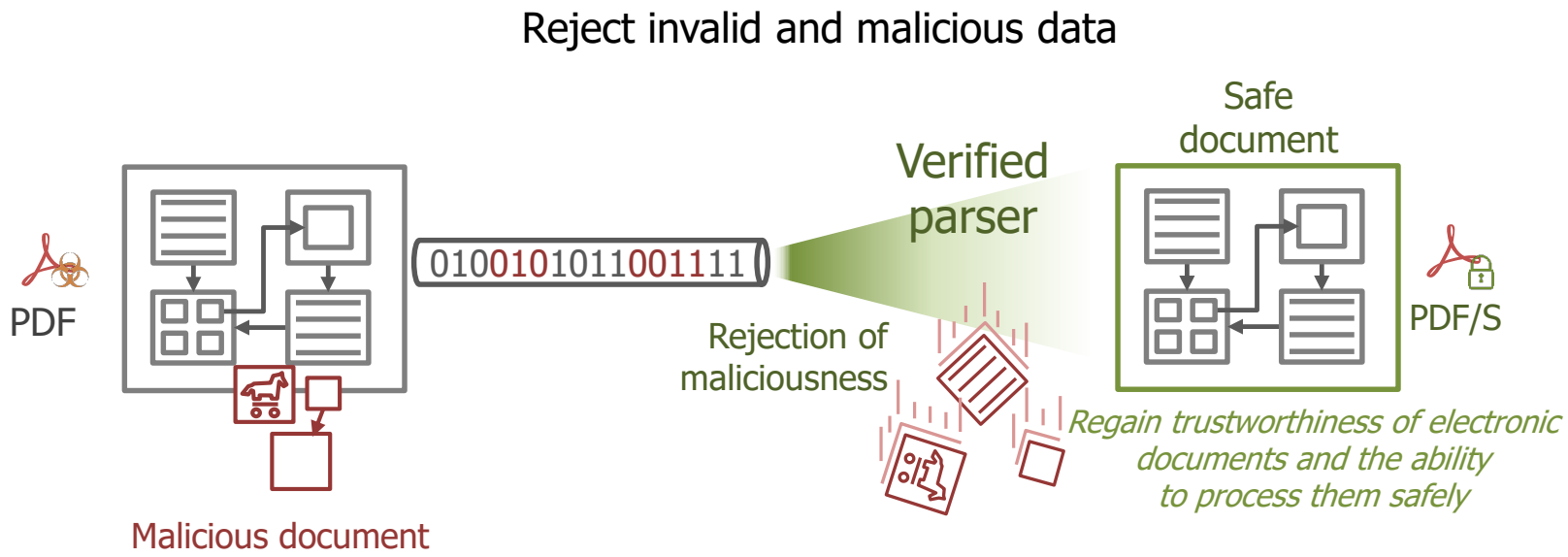
Skilled red teams were unable to compromise HACMS hardened platform



- Inserted mathematically-analyzed secure software kernel underneath mission computer software
- Added secure components to replace security-critical elements of the existing Unmanned Little Bird software

Verified secure Boeing Unmanned Little Bird

Ingesting data safely

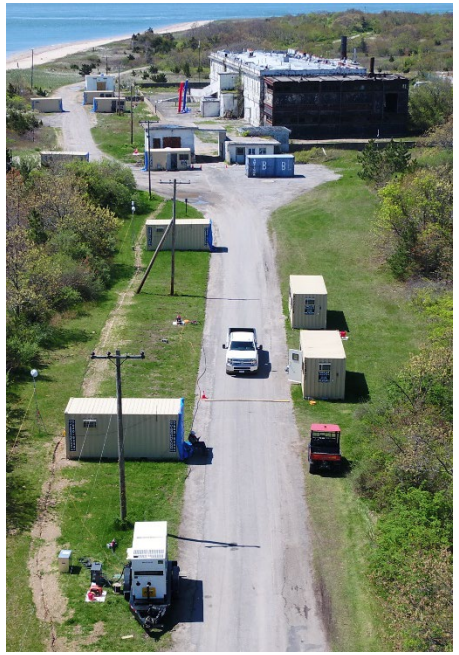


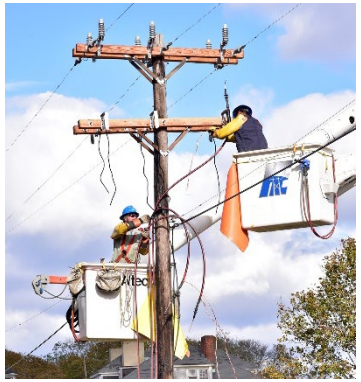
Safe Documents (SafeDocs)

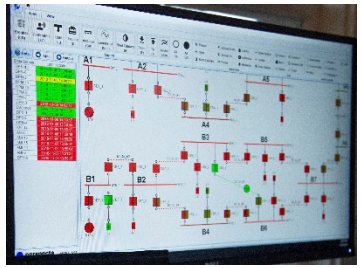
Accomplishments

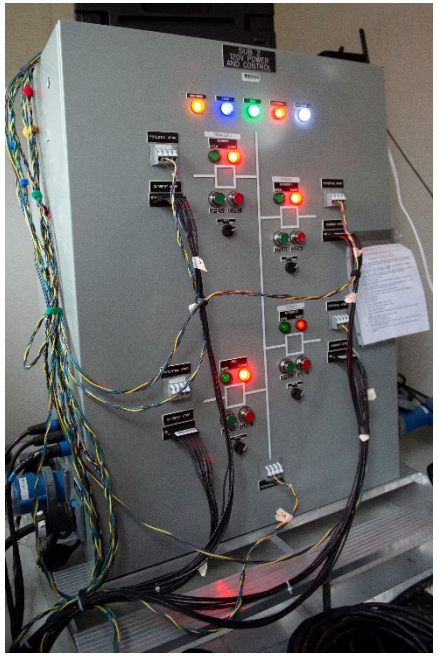
- Developed machine-readable descriptions and secure parsers for National Imagery Transmission Format (NITF), core structure of PDF, Air Vehicle Standard Interface (AVSI), Micro Air Vehicle Link (MAVLink)
- Developed tools to classify complex data objects as malicious or have violated standards
- Standards organization accepted 100 disambiguating edits into the ISO 32000-2 (PDF 2.0) International Standard
- Discovered a zero-day vulnerability in PDF digital signature handling across numerous workflow implementations

Black-start recovery of the electric power grid during a cyber attack

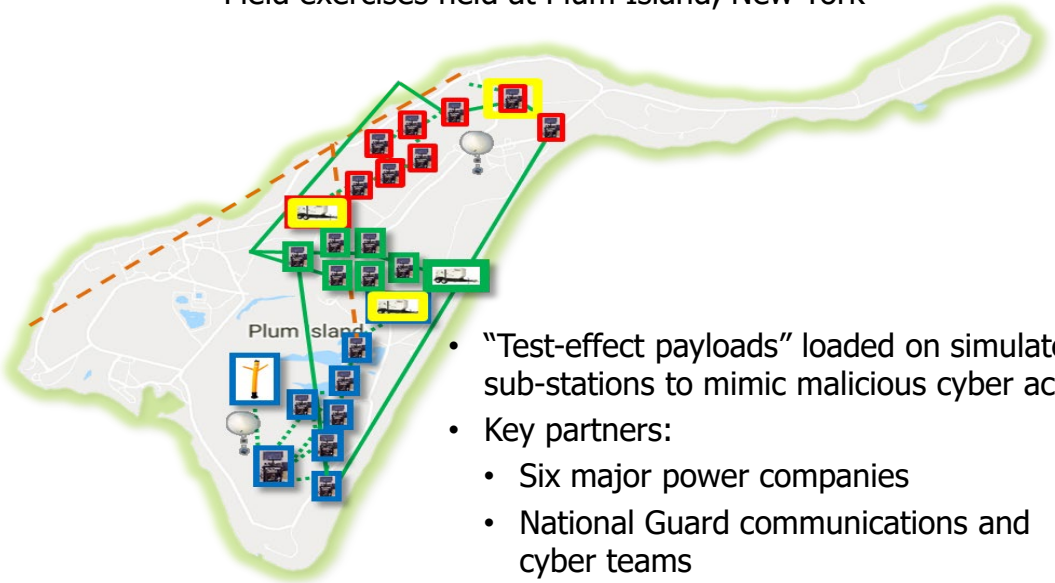








Field exercises held at Plum Island, New York



- "Test-effect payloads" loaded on simulated sub-stations to mimic malicious cyber actors
- Key partners:
  - Six major power companies
  - National Guard communications and cyber teams
  - Department of Energy
    - Liberty Eclipse partner

Rapid Attack Detection, Isolation and Characterization Systems (RADICS)

Accomplishments

- Developed grid sensing tools to identify cyber attacks
- Demonstrated isolation of compromised communication channels and nodes
- Developed secure emergency network communications
- Demonstrated a cyber weapon hunting system integrating traffic analysis, SCADA and IT protocol inspection, telemetry power reasoning, device configuration inspection, binary code behavior analysis, and RF emanation anomaly detection
- Demonstrated remote forensic analysis capability to analyze relays, energy controllers and networks

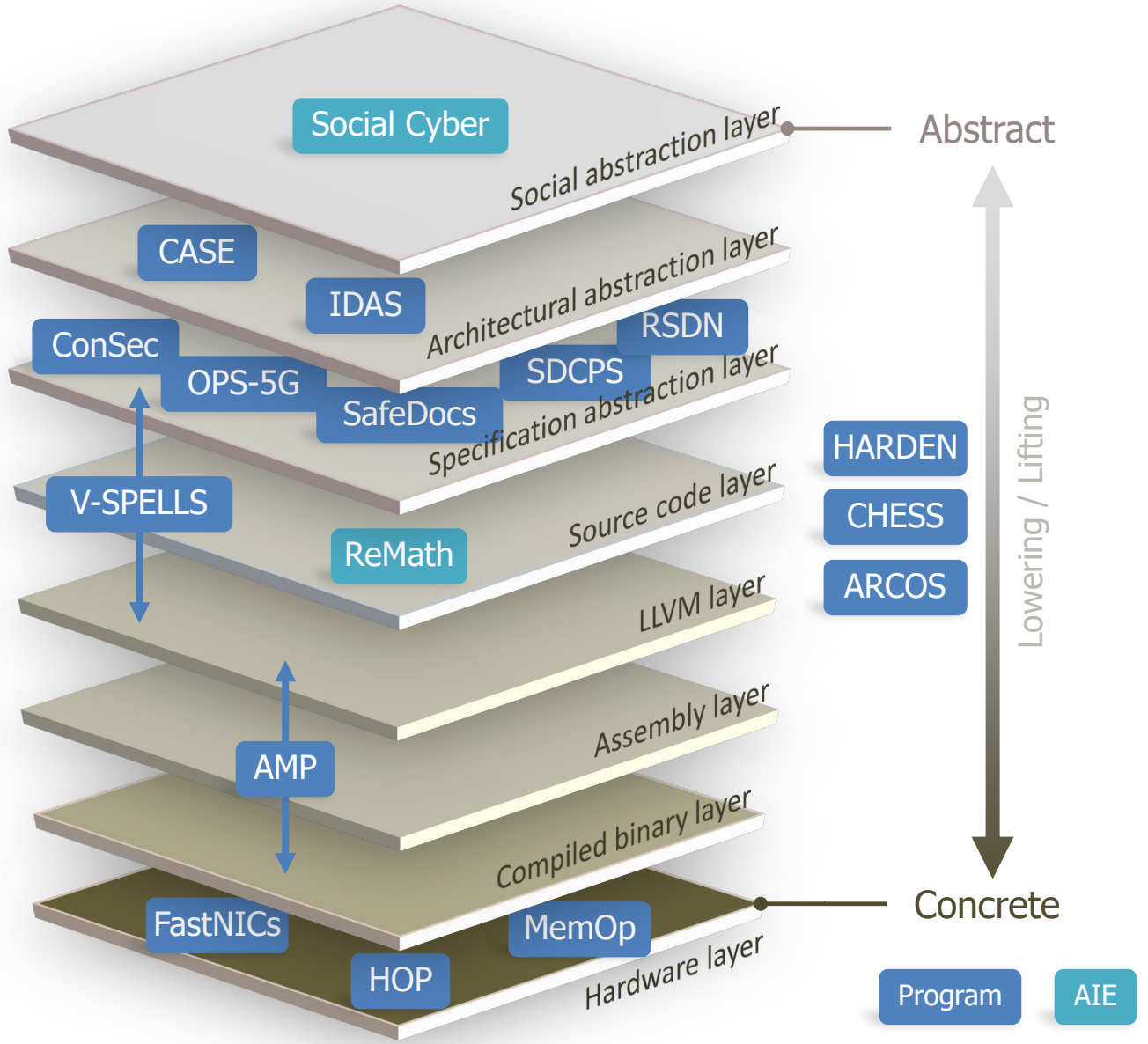
Resilient, adaptable, and secure systems

Goal

- Reduce our attack surface
- Enable faster development and deployment of high-quality software systems

Approach

- Build our systems with proofs of correctness
  - Verify properties using formal methods and models
- Develop high-assurance computing architectures
- Leverage AI/ML to scale faster
- Track software origins and create transparency
  - Enable information integrity via data provenance
  - Mine binaries, legacy code, and social forums
- Continuously collect artifact-based evidence for assured test & evaluation and certification



AMP: Assured Micropatching
ARCOS: Automated Rapid Certification Of Software
CHESS: Computers and Humans Exploring Software Security
ConSec: Configuration Security
CASE: Cyber Assured Systems Engineering
FastNICs: Fast Network Interface Cards
HARDEN: Hardening Development Toolchains against Emergent Execution Engines
HOP: Hardware Optimization
IDAS: Intent-Defined Adaptive Software

MemOp: Memory Optimization
OPS-5G: Open, Programmable, Secure 5G
ReMath: Recovery of Symbolic Mathematics from Code
RSDN: Resilient Supply-and-Demand Networks
SafeDocs: Safe Documents
SDCPS: Symbiotic Design for Cyber Physical Systems
Social Code: Hybrid AI to Protect Integrity of Open Source Code
V-SPELLS: Verified Security and Performance Enhancement of Large Legacy Software