Supply Chain Dilemmas

William Scherlis
Director, DARPA Information Innovation Office (I2O)

C3E

October 2021

Information Innovation Office (I2O)

Advantage in **cyber operations**

Proficient **artificial intelligence**

Resilient, adaptable, and **secure systems**

Confidence in the **information domain**

Cyber defense

Engage

- Systems and networks
- Humans
- Rapid response

Detect

- Monitors and logs
- Forensics
- Hunt, attribute

Prevent

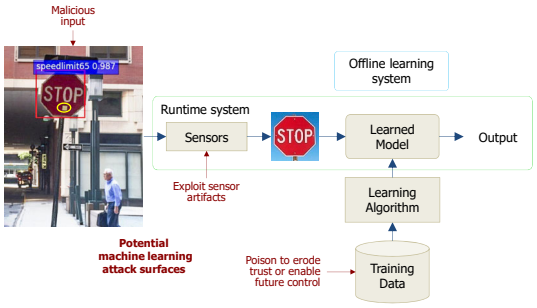
- Cyber hygiene
- Find potential accesses
- Design and architecture
- Protect data and software
- Secure networks
- Design for evaluation

Supply chain dilemmas

- Design and engineering
  1. AI assurance
  2. Abstractions
  3. Architecture
  4. Evidence
- Operations
  5. Opacity
- Supply chain
  6. Data and analytics

Guaranteeing AI Robustness against Deception (GARD)

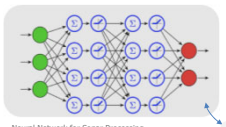
Develop theoretical foundations, principled defense algorithms, and evaluation frameworks to enable machine learning systems to be robust against adversary deception



Source: https://engineering.nyu.edu/news/seeking-new-element-artificial-intelligence-trust

Assured Autonomy

Develop rigorous design and analysis technologies for *continual assurance* of *learning-enabled autonomous systems*, in order to guarantee *safety properties in adversarial environments*



- Explain
- Analyze/assure
- Demo UXV operation

Function & safety cases

... (n == 5 + m) v (p ∧ ¬q) ...

SMT solver

SMT: Satisfiability modulo theories

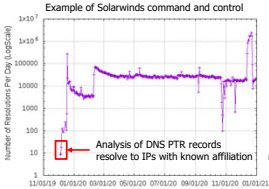
Cyber – key operational elements

Example of emergent behavior from design

Access

Hardening Development Toolchains against Emergent Execution Engines (HARDEN)

Example of Solarwinds command and control



C2

Enhanced Attribution (EA)

Example of infrastructure protection and recovery

Effects

Rapid Attack Detection, Isolation and Characterization Systems (RADICS)

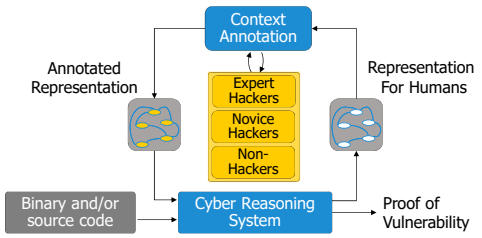
Hiding

Harnessing Autonomy for Countering Cyberadversary Systems (HACCS)

www.aoc.gov/explore-capitol-campus/art/about-national-statuary-hall-collection

Computers and Humans Exploring Software Security (CHESS)

Develop computer-human systems to rapidly discover all classes of vulnerability in complex software



Challenges
- Identify and generate representations that communicate information gaps to humans
- Capture and reason over the representations
- Extend CRS technology to scale up and reason over new and existing representations

Accomplishments
- Prototype CHESS system has been used to find and responsibly disclose vulnerabilities in real-world software
  - Five critical vulnerabilities in Adobe software products affecting over 1 billion devices
  - 103 vulnerabilities in NodeJS affecting over 55% of all downloaded Node JS packages (4.5M / week)

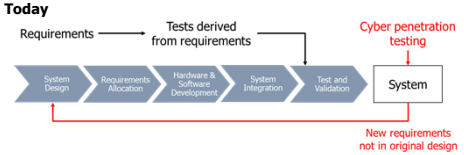
Software systems technical architecture

- Elements of technical architecture
  - Constraints on structural features of a system
  - Constraints on semantic features of a system
  - Rules of engagement among system elements
    - Components and services
    - Structured data exchange
- Goals
  - Loose coupling – enable separation of activities
  - Encapsulate variabilities – reduce interdependencies
  - Anticipate change – minimize re-engineering
  - Design for qualities – enhance performance, security, safety, etc.
- Principles
  - Minimal
  - Designed for evolution
  - Modeled and analyzable

Cyber Assured Systems Engineering (CASE)

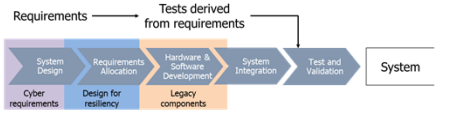
Develop advanced design and analysis tools that establish cyber resiliency as an explicit property for complex cyber physical systems

Today



Challenges
- Cyber issues are not well addressed by systems engineering practice
- Penetration testing is needed for design discovery
- Resiliency relies on hardening, late in process

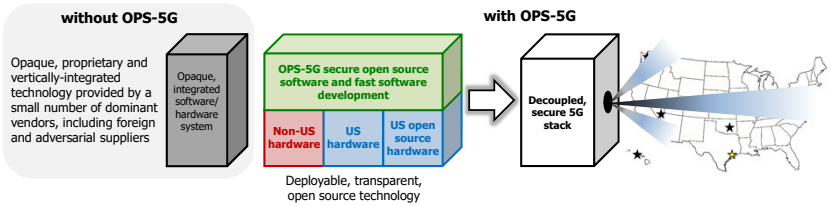
CASE



Approach
- Derive cyber requirements for resiliency early in design
- Apply semantically-rich modeling and analysis as part of the systems engineering process
- Adapt legacy software to support system resiliency

Open Programmable Secure 5G (OPS-5G)

Create open source software and systems enabling secure 5G and subsequent mobile networks



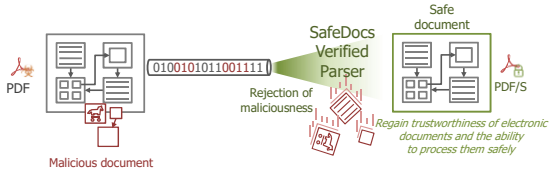
Challenges:
- Hardware/software decoupling
- Security at scale
- Operating over untrusted nodes and nets
- Adaptive adversaries at tera-node scale

Approach:
- Speed open source software development
- Built-in, cost-effective 5G node and network security
- Secure slices operate over untrusted infrastructure
- Programmable defenses for quick and flexible response

Transition:
- The Linux Foundation
  - Technology transfer path to military and civilian users
- Nationwide network to enhance DoD ability to test 5G Core security
  - Multisite OPS-5G Joint Independent Testing Option (MOJITO)

Safe Documents (SafeDocs)

Reduce electronic document attack surface and build verified parsers to radically improve software's ability to reject invalid and malicious data

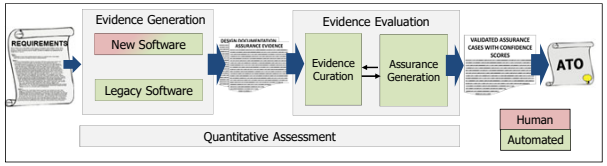


Approaches
- Develop accessible ways of programming parsers to **increase resiliency** and **reduce attack surface** of parsers
- Create unambiguous **machine-readable, human-intelligible** descriptions of de facto data formats
- Deduce **safe format subsets** for DoD uses
- Create **tools** for DoD experts to rapidly implement analyzers for data formats, and respond to malformations

Accomplishments
- Tooling that (1) helps detect and characterize novel and implicit format extensions and (2) ingests and characterizes malformations in a format sample corpus
- Secure parsers and machine-readable descriptions for National Imagery Transmission Format (**NITF**), core structure of **PDF**, Air Vehicle Standard Interface (**AVSI**), Micro Air Vehicle Link (**MAVLink**)
- PDF standard repairs – 50 disambiguating edits accepted into the ISO 32000-2 (**PDF 2.0**) International Standard

Automated Rapid Certification of Software (ARCOS)

Automate the evaluation of software assurance evidence to enable certifiers to rapidly determine that the risk of software deployment is acceptable



VS.

Global Hawk operations were based on (and limited by) a Certificate of Waiver or Authorization

ATO: Authority to Operate

Enhancing the Nation's Cybersecurity

Federal Register
Vol. 86, No. 93
Monday, May 17, 2021

Presidential Documents

Title 3—
The President

Executive Order 14028 of May 12, 2021

Improving the Nation's Cybersecurity

By the authority vested in me as President by the Constitution and the laws of the United States of America, it is hereby ordered as follows:

Section 1. *Policy.* The United States faces persistent and increasingly sophisticated malicious cyber campaigns that threaten the public sector, the private sector, and ultimately the American people's security and privacy. The Federal Government must improve its efforts to identify, deter, protect against, detect, and respond to these actions and actors. The Federal Government must also carefully examine what occurred during any major cyber incident and apply lessons learned. But cybersecurity requires more than government action. Protecting our Nation from malicious cyber actors requires the Federal Government to partner with the private sector. The private sector must adapt to the continuously changing threat environment, ensure its products are built and operate securely, and partner with the Federal Government to foster a more secure cyberspace. In the end, the trust we place in our digital infrastructure should be proportional to how trustworthy and transparent that infrastructure is, and to the consequences we will incur if that trust is misplaced.

...

(vii) providing a purchaser a Software Bill of Materials (SBOM) for each

...

(ii) develop a plan to implement Zero Trust Architecture, which shall

...

Software/system supply chains – what's in the bill of materials?

Diverse elements, often diversely sourced…

- *Vendor components* (opaque or transparent)
- *Custom components* (opaque or transparent)
- *Networked services* (opaque or transparent)
- *Open source components*
- *Tool chains, DSLs, generators* (opaque and transparent)
- *Glue*
- *Architectural elements*

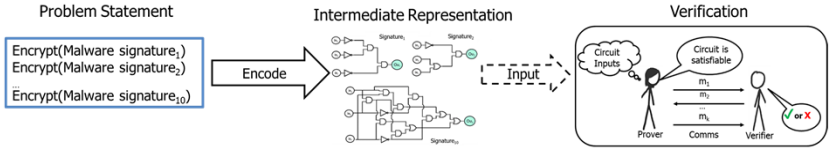
Some challenges…

- *Blurred boundaries*
- *Extends beyond scope of control*
- *Opacity*
- *Hidden correlations*

Securing Information for Encrypted Verification and Evaluation (SIEVE)

Develop computer science theory and software to create mathematically verifiable public statements derived from hidden, sensitive information in order to publically yet securely communicate about DoD capabilities

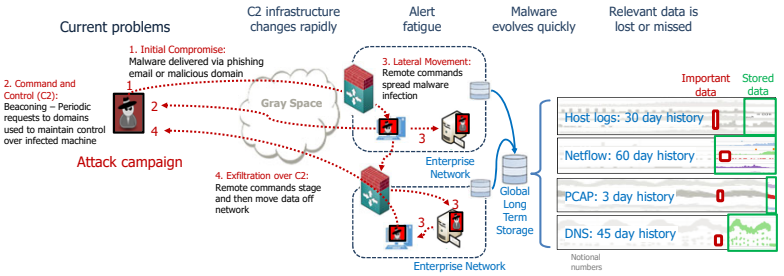
Zero Knowledge Proofs: Enable verification while keeping secrets



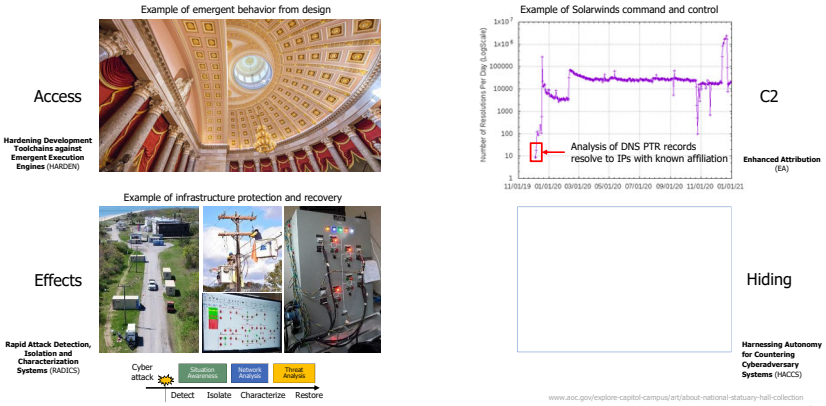
Accomplishment: Demonstrated the first-ever capability to mathematically prove the exploitability of vulnerable software without revealing critical details of the vulnerability or of the exploit

Cyber-Hunting At Scale (CHASE)

Automate cyber hunting via adaptive data collection at DoDIN scale



Cyber – key operational elements



Enhanced Attribution

Collect and fuse all available sources of information to enable continuous tracking of cyber adversary threat groups and individual operators