Cyber Security at the SEI

26 September, 2017

Software Engineering Institute

A DoD R&D FFRDC operated by Carnegie Mellon University

Mission

To support the Nation's defense by advancing the science, technologies, and practices needed to acquire, develop, operate, and sustain software systems that are innovative, affordable, trustworthy, and enduring

Approach

- Research
- Collaboration
- Development and Demonstration
- Transition

SEI works to address gaps in 7 technical areas

Enduring

Software Engineering & Information Assurance

Enable high quality, secure software-based systems in a predictable, affordable manner

Cyber Security

Develop improved systems, repeatable practices, and capable personnel to enable cyber missions

System Verification & Validation

Enhance confidence in the systems engineering lifecycle with evidence-based methods and tools

Make software less costly and more resilient and mission capable by ruthlessly automating all aspects of design, development, integration, testing, deployment, operations, defense, and sustainment of software systems

Emerging

Data Modeling & Analytics: Develop and apply mathematically rigorous data collection, analysis, and visualization techniques

C4ISR Mission Assurance: Enable reliable and predictable mission support by software and systems, which are resilient to adversary actions

Autonomy & Counter-Autonomy: Develop evidence that indicates the trustworthiness, dependencies, & vulnerabilities of autonomous systems

Human-Machine Interactions: Invent, assess, improve comprehensible, safe, and trustworthy technologies for humans to use and team with machines

CERT

Anticipating and solving the Nation's cybersecurity challenges

Enabling

Acquirers & Developers

Operators & Analysts

Decision Makers

Acquirers & Developers

Operators & Analysts

Decision Makers

Security-Aware Acquisition

Secure Development

System and Platform Evaluation

Threat-Aware Sustainment

Enterprise Risk Management

Network Situational Awareness

Cyber Intelligence

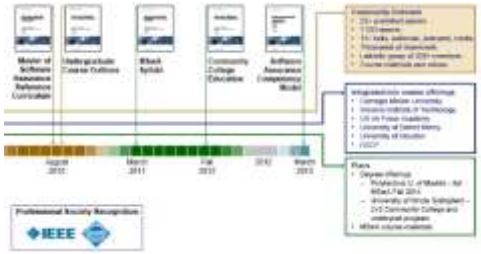
Digital Forensics

Insider Threat

Cyber Operator Development

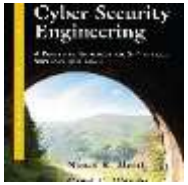
Cyber Center Development

Security-Aware Acquisition



COCOMO® II

ASQUARE
Security Quality Requirements Engineering for Acquisition



Addressing vulnerabilities and planning for threats earlier or more effectively in the lifecycle

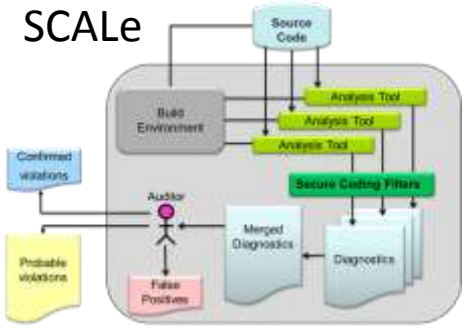
Current

- Improving security requirements elicitation
- Operationally informed threat modeling
- Development-time evidence useful for accreditation
- Refining cost estimation of security controls
- Recommended contract language for measurable performance
- Assessing and predicting software assurance capabilities

Future

- Reusable secure architecture patterns

Secure Development



CERT Secure Coding Professional Certificates

Assuring and assessing platforms through the analysis of source code

Current

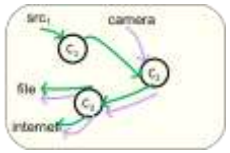
- Language-specific coding standards with automated enforcement
- Composition of static analysis capabilities
- Automated domain-specific code rewriting
- Architecture recovery
- Program correctness through model-checking
- Integrating security into Agile and DevOps

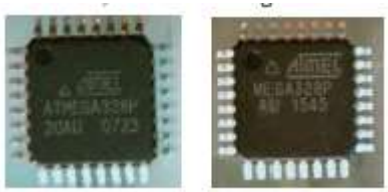
Future

- Coverage of additional languages
- Comprehensive automated source code rewriting

System and Platform Evaluation

DidFail





Assessing software, devices, systems and platforms of unknown design or provenance

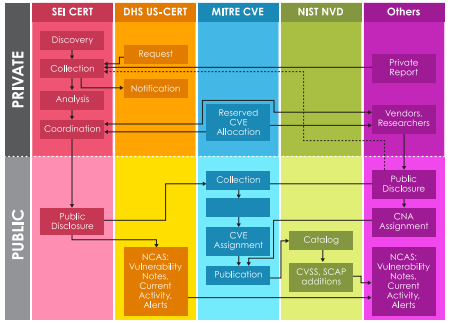
Current

- Repeatable approaches to find classes of vulnerabilities
- Focused analysis of features, behaviors, attack surface and implementation
- Automated characterization of capabilities or functionality
- Characterize the relationships between defects and vulnerabilities

Future

- Automated PoC exploit generation

Threat-Aware Sustainment



Reducing the window of exposure from known vulnerabilities in fielded systems

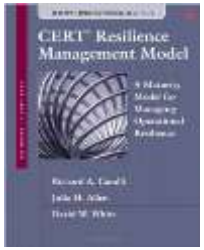
Current

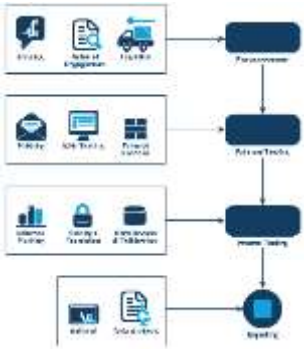
- Vulnerability coordination
- Timely watch-and-warning of new vulnerabilities and recommended mitigations
- Identifying systemic problems and emerging trends
- Guidance on establishing and operating a Product Computer Security Incident Response Team (PCSIRT)

Future

- Application and refinement of existing methodologies to new software ecosystems

Enterprise Risk Management





CSP FLIPBOOK

Carnegie Mellon University CIO Institute

Measurable practices and frameworks that enable an organization to measure and mitigate risk

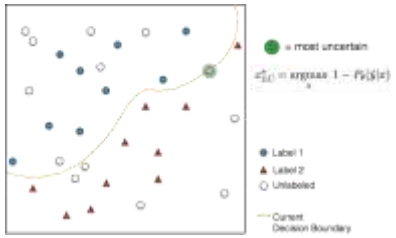
Current

- Guidance on industry and government compliance and commonly-accepted practices
- Assessment approaches to identify capabilities and maturity
- Predicting security posture through practice and process evaluations, risk assessments and technical control data
- Economic models to prioritize investments and quantify their effectiveness

Future

- Cyber Maturity Model

Network Situational Awareness



Reasoning about the cyber terrain in context of the mission

Current

- Sensors that maintain visibility into the evolving network and platform technologies
- Analytical techniques that synthesize organizational, grey-space and cyber intelligence data to:
  - Characterize assets at risk
  - Measure scope and scale of adversary activity
  - Prioritize response to threat data
  - Resource planning and provisioning

Future

- Improved insight into the cyber-dependencies
- Cyber affordances

Cyber Intelligence

Pharos Framework

+

ROSE@LLNL

The Cyber Intelligence Research Consortium

Emerging Technology Center

Characterizing the behavior, capabilities and properties of adversary cyber tools and actors

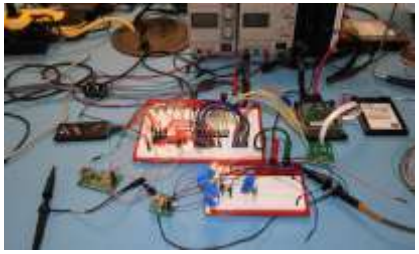
Current

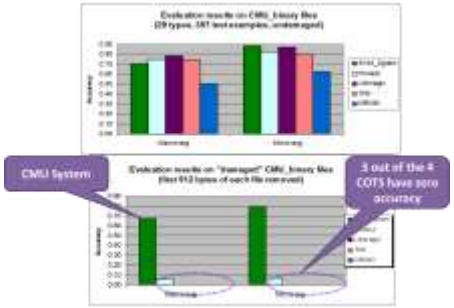
- Automation for reverse engineering
  - Deobfuscation and unpacking
  - Code comprehension
  - Dynamic analysis environments
- Creating indicators and identifiers for the detection and attribution of actors and malware families
- Trending emerging capabilities, tactics and targets
- Enabling threat modeling for system design

Future

- Automated code comprehension
- Automated malware classification

Digital Forensics





Enabling incident response and analysis activities as the technology and adversary evolves

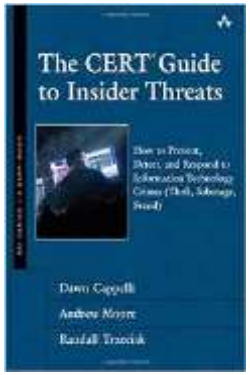
Current

- Forensic recovery techniques for data on emerging mediums
- Models to evaluate the efficacy of cyber effects and mitigations

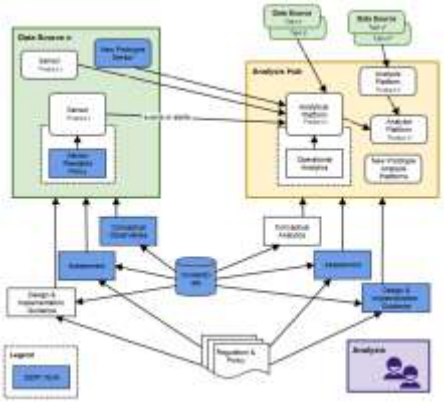
Future

- Increased capabilities in the analysis of:
  - Crypto-currencies and related infrastructure
  - Mobile application ecosystem

Insider Threat



CERT Insider Threat Certificates and Training



Detecting and mitigating the impact of and reducing the likelihood of insider threat

Current

- Indicators to use in end-point and hub analytics
  - Reactive – user activity monitoring
  - Proactive – behavior modelling
  - Preventative – aids and incentives
- Guidance on establishing and operating insider threat programs compliant with the EO 13587 and NISPOM

Future

- National Insider Threat Research Development Testing and Evaluation Facility

Cyber Operator Development

Growing and maintaining a cyber workforce at sufficient scale with a known readiness

Current

- Designing and executing of Joint and Service-scale exercises
- Representative cyber environments for modelling and simulation
- Verifying role readiness of cyber operator
- Federated architecture to link cyber and kinetic simulators

Future

- Automated assessment of operators
- Improved trainee engagement through gamification

Cyber Center Development

Measurable and repeatable practices to improve and align operational security organizations

Current

- Models to guide investments and organization processes based on emerging threats, technology landscape and mission priorities
- Analytics of workflow data
- Automated information sharing
- International capability building

Future

- Improved capacity and capability models

Transitioning Capability from the Lab to the Field

Analysis **Prototypes** **Training**

www.cert.org

CMU SEI 2017 Research Review: October 17-18

An annual event held in Pittsburgh featuring presentations and posters session describing the results of our FY Line-funded research projects.

In our 2017 Research Review, you will learn about AR&D conducted during FY2017 concerning automated code repair, causal factors of software cost, machine perception, cyber workforce training, continuous runtime verification, and other areas important to closing technology gaps across the software lifecycle.

The CMU SEI 2017 Research Review is by invitation only. The event is free, but we do ask that you register. The full program and registration is available on the event site http://www.sei.cmu.edu/go/research-review/index.cfm

If you have any questions or would like to attend contact Palma Buttles pjb@sei.cmu.edu

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8721-05-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.