

Methodology for Assessment of Security Properties

Cyber Security Division 2012 Principal Investigators' Meeting

October 9 - 11, 2012

Cynthia E. Irvine
Professor of Computer Science
Naval Postgraduate School
irvine@nps.edu
831-656-2461

Introduction

- Project: *Methodology for Assessment of Security Properties*
 - Principles → methods → assessment framework / tools
- Addresses TTA 5 Goals
 - Survivability
 - Methodology supports assessment security architecture
 - Coherent security architecture → self protection
 - Large-scale consequences
 - SCADA is target of framework and testing phase
 - Availability of tools potential for broad SCADA security enhancement
 - Security and resilience
 - Central properties of assessment framework

Introduction

- Maintain secure states
 - Complex systems mapped to security models
 - Models provide evidence of secure state maintenance
- Survivability against malware: Protect and Detect
 - Methodology includes assessment for
 - Balance of security and availability
 - Ability for self protection
 - Defense in depth and redundancy
 - Modeling for ability to continue operations
 - Ability to audit security actions
 - Self protection

Introduction

- Adequate requirements for survivability
 - Methodology supports reasoning about the relationship of requirements to security goals
 - Identification of trusted computing base ensures that the core components have sufficient assurance

Introduction - Team

- PI: Cynthia E. Irvine
- Timothy Levin, Security Engineer
- Thuy Nguyen, Security Engineer
- Team Project History Samples
 - CyberCIEGE: US Navy, NSF, OSD
 - TCX: ONR, NRO, OSD
 - 3Dsec and RCsec: NSF
 - Secure Core: NSF
 - SKPP: NSA
 - MSHN: DARPA
 - MYSEA: NRO
- Over 75 years of collective experience
 - Analysis, design and development of secure systems
 - Systems requirement analysis

Problem Scope

- National control infrastructure largely unprotected
- State-sanctioned cyber attacks are a reality
 - Stuxnet, etc.
 - Bilateral, asymmetrical
- We lack metrics to assess cyber security, e.g. architectures
- Large scale replacement is cost prohibitive
- We lack techniques for composite development
 - e.g., insertion of key “policy enforcement” components

“We do not understand how to combine systems in ways that ensure that the combination is more, rather than less, secure and resilient than its weakest components”

- A Roadmap for Cybersecurity Research, DHS, 2009.

Technical Solution

- Develop a taxonomy of principles for secure composite systems
- (SCSs) Securing of complex systems based on
 - Coherent security architecture
 - Keystone components
 - Principles for composition
 - Reusability of components
 - Potential for infrastructure overhaul
- Translate the principles into a systematic methodology for assessment of secure composite systems
- Adapt the methodology specifically to a SCADA Security Assessment Framework

Technical Approach

- Gathering of information and tools
 - Extraction, refinement, extrapolation and integration of key ideas into a set of principles and usage guidelines.
 - Explore use of of formal language to provide syntactic rigor
- Organization of principles into a methodology for security-preserving modular composition
 - Design of sequential and stand-alone procedures for:
 - Integration of components into systems
 - Assessment of systems and properties
 - Reduction to metrics
 - Focus on SCADA and ICS architectures

Technical Approach

- Framework
 - Develop *tool* for composition analysis and exploration
 - Apply tool to a SCADA system – case study
 - Examine results to assess efficacy of methodology
 - Finding flaws in target systems
 - Development of alternative methods and counter-designs
 - Utility of metrics

Technical Challenges

- Translation of principles into systematic methodology
 - Lack of composition/decomposition support in modern guidelines
 - Legacy guidelines lack rigorous foundation and are difficult to understand and apply
 - Identification of pertinent system properties
 - Subsequent quantification
 - Development of security metrics difficult
- Derivation of assessment framework & composition tools from procedural methods
 - Automation may be difficult
 - Access to authentic SCADA systems and vulnerabilities

Milestones, Deliverables & Schedules

- Reports describe achievement of key milestones
 - 9 mos.: Organization and taxonomy
 - 15 mos.: *Preliminary Rules for Composing Secure Systems*
 - 24 mos.: *Methodology for Analysis of Secure Composite Systems*
 - 30 mos.: *Automated Analyzer of Secure System Composition*
 - *Including devices with cyber-physical interfaces*
 - 36 mos.: *Assessment of Methodology for Analysis of Secure Composite Systems*
 - Case Study of application to SCADA
- Publish papers derived from key achievements

Technology Transition Plan

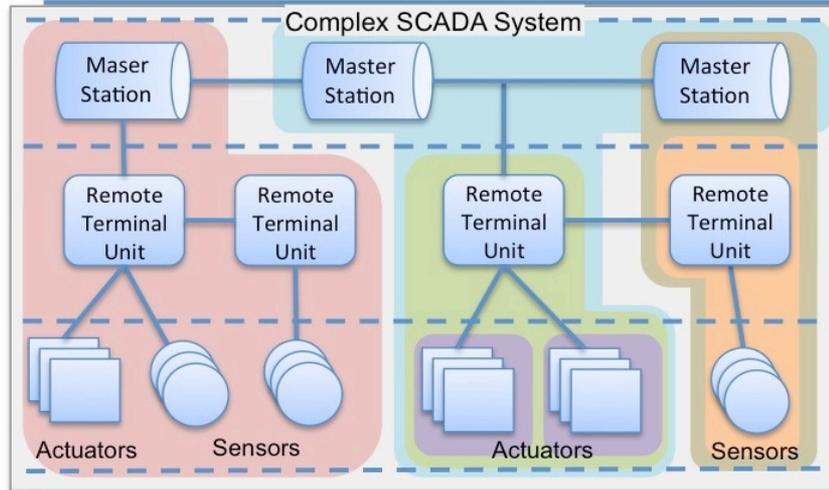
- Secure system composition tool produced during assessment phase
 - Open source availability* on completion of project:
 - Tool
 - Methodology report
 - Examples and test results
 - Also available for commercialization for:
 - Customer support
 - Product maintenance and enhancement

* *Calhoun archiving system at NPS Library*

BAA Number: Cyber Security BAA 11-02

Title: *Methodology for Assessment of Security Properties*

Offeror: Naval Postgraduate School



Proposed Technical Approach:

1. Our goal is to address the challenge of composing secure systems from heterogeneous components having different security characteristics. We will apply basic cybersecurity science to identify and reason about properties relevant to composed secure systems. We will create a methodology and assessment framework that ensures properties such as resilience are supported structurally, and avoids single points of failure. Other key attributes will include auditing, self-diagnosis and self-protection capabilities.
2. Basic tasks are to (a) develop a taxonomy of principles for secure composite systems (SCSs), (b) translate the principles into a systematic methodology for system assessment, and (c) adapt the methodology specifically to a SCADA Security Assessment Framework.
3. Our related work: we were lead analysts for the Separation Kernel Protection Profile; we previously constructed a comprehensive list of modern system security principles. Also supervised various SCADA theses and research projects.

Operational Capability

1. Performance targets: (a) Incorporation of major composition principles from the existing literature and identification of new composition rules and algorithms; (b) Translation of principles and algorithms into usable methodology; (c) Adapt methodology to *assessment framework*
2. Performance for key parameters: (a) Coverage of all relevant principles, newly identified and from the literature; (b) Methodology includes all relevant of principles (c) Framework is applicable to 75% of major SCADA systems
2. The cost of ownership relates to the effort extended to apply the framework to target systems.
3. Methodology ensures a *coherent* system and network security architecture for which maintenance of *secure state* and a *resilient posture* is readily apparent through security by design.

Schedule, Cost, Deliverables, & Contact Info:

Milestone decision points: 3 distinct phases

Period of performance: 3 years

Phase 1: 18 months

Phase 2: 12 months

Phase 3: 6 months

Deliverables: (1) Principles for Secure Composite Systems (SCSs),
(2) Methodology for construction of SCSs, and
(3) SCADA Security Assessment Framework

Corporate Information: Naval Postgraduate School

POC: Technical

Administrative

Name: Cynthia Irvine

Danielle Kuska

Addr: 1 University Circle
Monterey, CA 93943

1 University Circle
Monterey, CA 93943

Phone: 831-656-2461 (irvine)

831-656-2099 (kuska)

E-mail: irvine@nps.edu

dkuska@nps.edu

Summary

- We lack methods and metrics to develop/assess cyber security
 - Large scale replacement is cost prohibitive
 - We lack techniques for composite development
- Approach: *Principles* → *Methods* → *Framework & Tools*
- Benefits: framework for composition analysis and exploration
 - Supports reasoning about survivability and security
 - Potential large-scale benefit of applying results to national scale SCADA environments

Questions & Comments

irvine@nps.edu

Backup Slides

Technical Approach

- Theory metrics x rules x templates \Rightarrow Methodology
- Methodology x legacy system x secure components
 \Rightarrow Coherent security architecture
- CSA x analysis tools x metrics \Rightarrow properties and policies
 - Security, Integrity, Survivability, Trustworthiness
 - Malware resistance
 - Adaptive policies for availability and security
 - Self protection, redundancy, audit
 - Security models
 - Secure states
 - Secure state changes