Cyber S&T Priority Steering Council
Research Roadmap
for the
National Defense Industrial Association
Disruptive Technologies Conference

8 November 2011
Steven E. King, Ph.D.
Problem Statement

Lack of trustworthiness:
Can’t trust global supply chain for mission-critical components

Lack of resiliency:
Inability to stop attack spread

Lack of agility:
Inability to maneuver and avoid attack

Lack of assured effective missions:
Missions impaired by cyber attacks

Lack of trustworthiness:
Can’t trust global supply chain for mission-critical components
Desired End State

Trusted foundations:
- Trusted design, verification, and fabrication of integrated circuits;
- Trusted boot and secure attestation

Assured effective missions:
- Missions success is ensured

Agile cyber operations:
- Maneuvering to avoid attacks

Resilient defenses:
- Ability to deflect, resist and absorb attacks

Evaluation of cyber vs. kinetic options

Mission success

External Cyber Attack

Insider Cyber Attack

Attacker neutralized

Attack deflected & absorbed

Diverting to Honeynet

APP
OS
BIOS

Verified ICs

Trusted boot
Key Parameter: Work Factor Ratio

• Missions
  – Kinetic, cyber, and combined missions will have a cyber dependency

• Infrastructure
  – Any element of the cyber infrastructure may be compromised and manipulated
  – DoD will continue to leverage commercial products and services we do not own or control
  – DoD infrastructure defies establishing an all-encompassing static perimeter

Challenge: Increase Adversary / Defender Relative Work Factor Over Time

Perimeter is not well defined
Four Major 10 Year Objectives

Assuring Effective Missions
Assess and control the cyber situation in mission context

Agile Operations
Dynamically reshape cyber systems as conditions/goals change, to escape harm

Resilient Infrastructure
Withstand cyber attacks, and sustain or recover critical functions

Trust
Establish known degree of assurance that devices, networks, and cyber-dependent functions perform as expected, despite attack or error
Metrics

Resilient Infrastructure

Restoration to Baseline Performance

- **Labor Required**
  - 2013: 100
  - 2018: 10
  - 2023: 1
  - *Automated: 1*

- **Days**
  - 2013
  - 2018
  - 2023

- **Hours**
  - 2013
  - 2018
  - 2023

- **Minutes**
  - 2013
  - 2018
  - 2023

- **Dynamic real-time reconstitution based on continuous feedback**

Operational Agility

- **Trust**
  - Log10 of the ratio of Foe-effort ($) to USG-effort ($)
  - 2013: Equal $ 9
  - 2018: 12
  - 2023: 15

- **Log10 of Complexity (Level, Scale of Trust)**
  - 2013
  - 2018
  - 2023

Assuring Effective Missions

- **Course of action option generation using cyber/kinetic situational awareness**
- **Predictive cyber/kinetic mission tools for use during live mission execution**

(Average Number of Cyber Specialists to Resolve a Significant Attack)
Trust Foundations

- Scalable reverse engineering and analysis
- Trust establishment, propagation, and maintenance techniques
- Measurement of trustworthiness
- Trustworthy architectures and trust composition tools
Resilient Infrastructure
Technical Challenges and Research Opportunities

Resilient Architectures
- Resiliency for operational systems
- Mechanisms to compose resilient systems from brittle components
- Integration of sensing, detection, response, and recovery mechanisms
- Secure modularization and virtualization of nodes and networks
- Resiliency-specific modeling and simulation

Resilient Algorithms and Protocols
- Code-level software resiliency
- Network overlays and virtualization
- Network management algorithms
- Mobile computing security

Large Scale Randomization

Application View
Platform View
Implementation View
Agile Operations
Technical Challenges and Research Opportunities

Autonomic Cyber Agility

- Techniques for autonomous reprogramming, reconfiguration, and control of cyber components
- Machine intelligence and automated reasoning techniques for executing courses of action

Cyber Maneuver

- Distributed systems architectures and service application polymorphism
- Network composition based on graph theory
- Distributed collaboration and social network theory
Assuring Effective Missions
Technical Challenges and Research Opportunities

Cyber Mission Control

• Techniques for mapping assets and describing dependencies between mission elements and cyber infrastructure
• Techniques for course of action development and analysis
• Cyber effects assessment
Open Broad Agency Announcements

- **Army Research Office (ARO)**
  - Solicitation #: W911NF-07-R-0003-04; BAA for Basic and Applied Research, Section 5.3

- **Army Research Laboratory (ARL)**
  - Solicitation #: W911NF-07-R-0001-05; BAA for Basic and Applied Research, Section 1

- **Communications and Electronics Research, Development, and Engineering Center (CERDEC)**
  - Solicitation #: W15P7T-08-R-P415

- **Office of Naval Research (ONR)**
  - Solicitation #: ONRBAA 12-001, Code 31 Section 1

- **Naval Research Laboratory (NRL)**
  - Solicitation #: BAA-N00173-02, Section 55-11-02 (Mathematical Foundations of Computing)
  - Solicitation #: BAA-N00173-02, Section 55-11-03 (High Assurance Engineering and Computing)

- **Air Force Office of Scientific Research (AFOSR)**
  - Solicitation #: AFOSR-BAA-2010-1, Section c.12

- **Air Force Research Laboratory (AFRL)**
  - Solicitation #: BAA-10-09-RIKA (Cross Domain Innovative Technologies)
  - Solicitation #: BAA-11-01-RIKA (Cyber Assurance Technologies)

- **Defense Advanced Research Projects Agency (DARPA)**
  - Solicitation #: DARPA-BAA-11-63 (Automated Program Analysis for Cyber Security)
  - Solicitation #: DARPA-BAA-10-83 (Strategic Technologies Office BAA)
  - Solicitation #: DARPA-BAA-11-34 (Information Innovation Office BAA)
  - Solicitation #: DARPA-RA-11-52 (Cyber Fast Track)
  - Solicitation #: DARPA-SN-11-55 (Future Directions in Cyber Security)

---

**Small Business Innovation Research Announcements**

http://www.dodsbir.net

**NSA Contact Information**
(No Open BAAs)

Acquisition Resource Center
Phone: (443)-479-9572
E-mail: nsaarc@nsaarc.net

Office of Small Business Programs
Phone: (443)-479-9572
E-mail: nsaarc@nsaarc.net
Technology Challenge Summary
POC: Dr. Steven E. King

Situational Awareness

Assuring Effective Missions
- Cyber Mission Control
- Effects at Scale

Agile Operations
- Autonomic Cyber Agility
- Cyber Maneuver

Resilient Infrastructure
- Resilient Architectures
- Resilient Algorithms and Protocols

Trust
- Trust Foundations

Fusion Instrumentation Sensing Observables
Metrics
Response
Effects Manipulation Controls Actuation

Figure is Unclassified