Computer Network Defense/ Information Assurance (CND/ IA) Enabling Capability (EC) Industry Day

BAA 10-004

Stanley Chincheck

Director,
Center for High Assurance Computer Systems

US Naval Research Laboratory
Code 5540
Washington, DC

stanley.chincheck@nrl.navy.mil

Agenda

- Technical Discussions
  - Overview
  - Key Technologies of Interest
  - Working Group
- BAA Overview
  - Few Issues of Note
  - Schedule/Critical Dates
- Break
- NCDOC Brief
- Contracts Brief
- General
  - Questions & Answers

How This is Going to Work….

- Today's Industry Day…
  - I will answer questions, however, I will not comment on a specific approach, technology, etc. being considered by an Offeror
  - I will not have separate meetings with any Offeror to discuss their "ideas, etc."
  - FAQ handed out, hopefully this will answer many of your questions
    - The response to any new questions today (on question sheets) will be captured on the updated FAQ
    - All materials today will be posted after the EC Industry Day on the ONR website

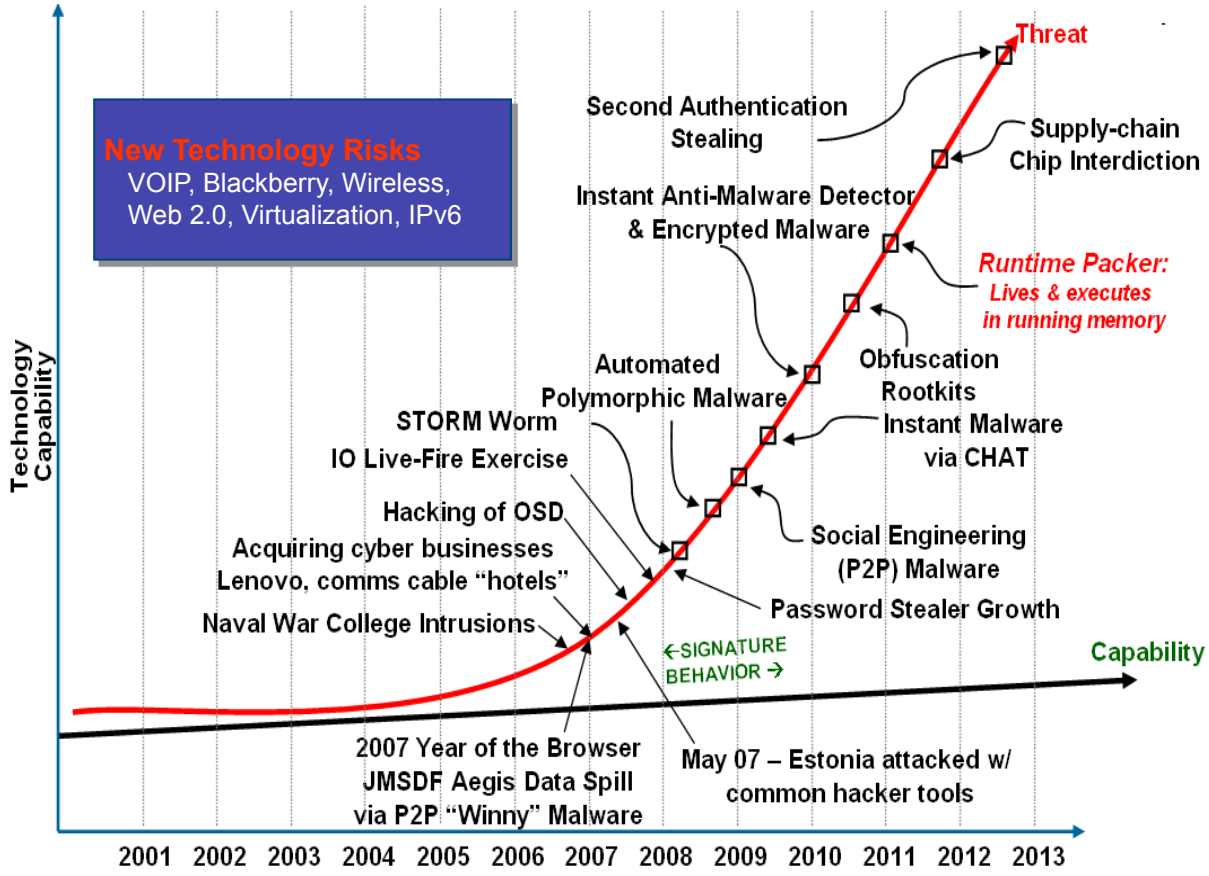
What is the Effort….
and Why….

What Has Changed…The Forcing Functions

- Previous strategy….
  - Focused on “keep the adversary out….”
  - “Defense-in-Depth”, worked for some…not others
- The environment has changed in the last 10 years
  - Ubiquitous computing
  - Pervasive globally connected networks...as well as convergence
  - Interactions have changed….coalition partners
- Why the Paradigm Shift
  - The adversaries are in….
    - We need to understand how they got in
    - Understand our adversary
      - Motivation, mindsets, etc…. different laws…reactions unpredictable
    - Shift away from “systems” view to an “enterprise” level view

Our Adversaries…Motivated…Capable

Linear Growth of MALWARE → **Variant MALWARE Explosive Growth**



New Technology Risks
VOIP, Blackberry, Wireless, Web 2.0, Virtualization, IPv6

New Hacker Capability
- 100 Malware Detections/Wk (2002)
- 2600 Detects per week (2007)
- 300% Malware increase (2008)
- 1 new Driver written every 4 minutes
- New Threat Vector:
  - Networking Technology
  - Encrypted Malware
  - Anti-Malware Detection
  - Foreign Language Malware
  - Black market PII Tools

Risks from Users
- Unauthorized software
- PCs on network,
- Flash drives, etc…
- Spillages
- Insider Threat

Signature-based defense of host A/V and network firewalls are ineffective
We need new ways to frame, understand and reverse these trends

CND/IA Enabling Capability Program

- Concept of Operations
  - Comprehensive, holistic approach to computer network defense (CND)
    - Not talking about IAVA compliance…or similar concepts that are actually *computer network management*
  - New paradigm, approach….it's all about mission execution
  - Critical technologies are to be developed with a "systems" approach
    - Not automating what we have today, what we do today, or how we do things today….fresh approach….purist viewpoint of "if I could wipe the slate clean and start over…."

CND/IA Enabling Capability Program

- Critical System Building Blocks
  - Sensors & Gateways
    - Components located throughout the network ensure network awareness by providing information regarding network traffic back to the decision support system
      - Dynamically reconfigurable over the network
      - Provide enhanced anomaly detection capabilities (e.g., beaconing activities, exfiltration, etc.)
      - Protect services/communication on network infrastructure to ensure essential network capabilities are provided
      - Provide robust security features for isolation and local mitigation actions

CND/IA Enabling Capability Program

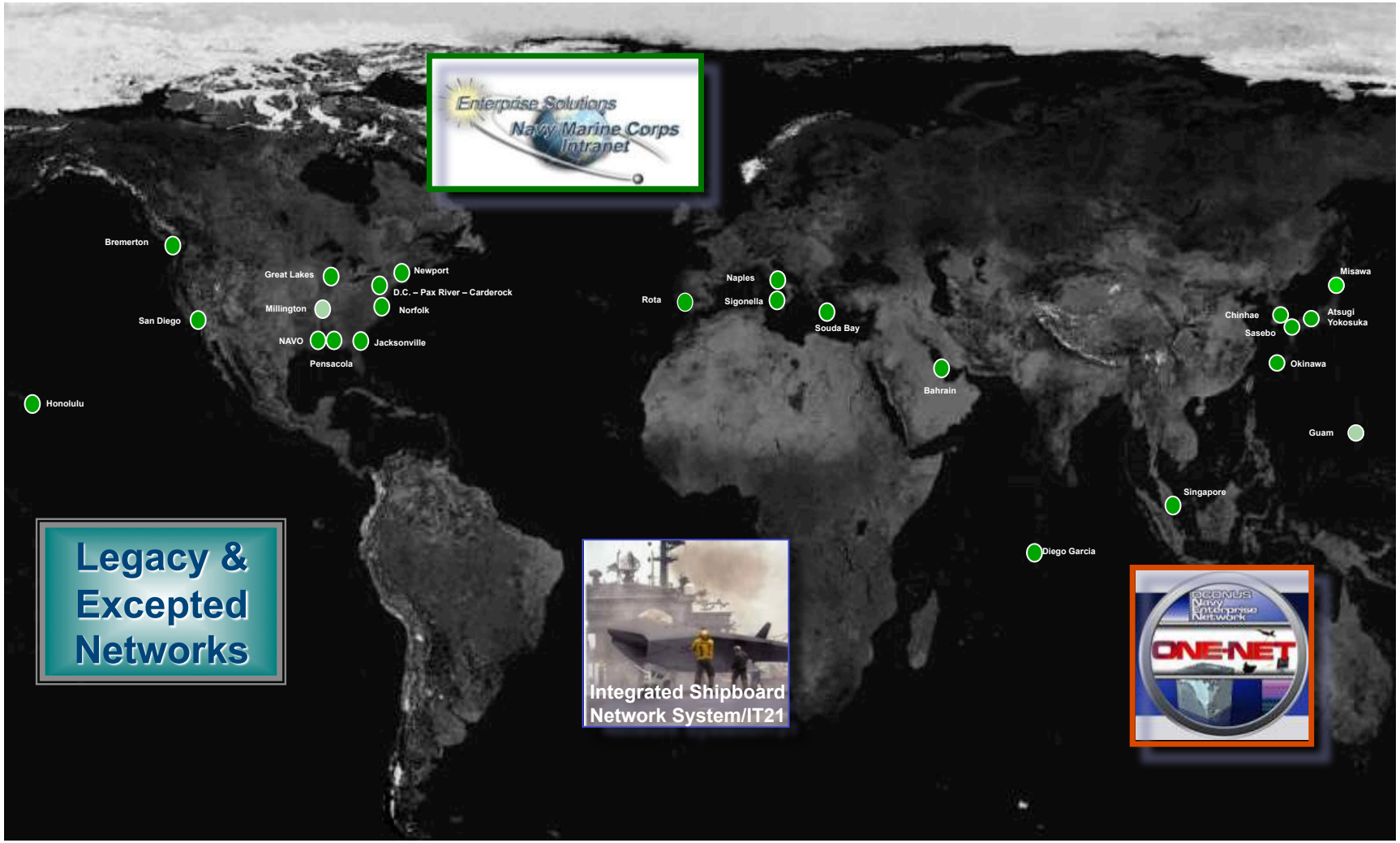
- Critical System Building Blocks
  - Common Operational Decision Support System
    - System that aggregates, correlates, fuses, and visualizes the network security posture information into a holistic view to support mission execution
      - “Cyber awareness" is supplemented using information provided by the sensors and gateways, and other network-based security components
      - Provides the real-time management and control of the sensors and gateways to support emergent requirements and to address near real-time network attacks
      - Provides to the user automated response capability up to a user specified threshold, and beyond that limit, provides recommended actions to the user

CND/IA Enabling Capability Program

- Critical System Building Blocks
  - Security Enabled Protocols
    - Hardened, dynamic and security-enabled
    - Data and control protocols to ensure data delivery, reliability and provenance
    - Provide configuration and control of network-based security components essential to mission operations
      - Support communications and security services that include data movement as well as asset management for functions such as enabling security features, blocking and filtering traffic, and collecting data for local analysis

Where Does This Apply….

Global Scale and Magnitude



CND/IA Enabling Capability Program

- Key Technologies of Interest
  - Algorithms
    - For malware detection (e.g., embedded in binary data files)
      - Techniques that discover malware entry points, encryption techniques, and self-obfuscation
      - Robust for expansion as malware techniques morph
    - To monitor network traffic
      - Capable of determining legitimate traffic from malicious network traffic
        - Beaconing, exfiltration, unauthorized in-bound data flows

CND/IA Enabling Capability Program

- Key Technologies of Interest
  - Algorithms
    - To support data mining and fusion of large-scale complex data sets
    - Supporting automated decision aides
      - Flexible thresholds
      - Threat isolation
  - Protocols to support both security and component management
    - Robust, providing data protection, management and control services
    - Providing protection against network-based attacks

CND/IA Enabling Capability Program

- Key Technologies of Interest
  - Methods for attribution
    - Support geo-location
    - Ability to identify targets of suspicious and potentially unauthorized network activity
  - Visualization of large-scale data sets
    - Near real-time
    - Input and process disparate data sources
    - Fusion and correlation

A Few Notes Regarding the Effort….

How This is Going to Work….

- White Papers
  - Offerors propose efforts addressing Key Technologies within their areas of expertise
    - Offerors can address more than one key technology area
      - However, all efforts must be rolled up into one White Paper
    - Must address the technology development and demonstration within their environment

How This is Going to Work….

- White Papers (cont.)
  - Both Phases must be addressed
    - Phase I
      - Requirements, architecture, concept
    - Phase II
      - Full scale development, testing, integration, etc.
- There is no intention to award to more than one vendor for “similar technology”
  - Not going to compete vendors
  - Want “best of breed”

How This is Going to Work….

- Government team is leading the Integrated Product Team (IPT)
  - Performance, interfaces, etc. defined within the IPT
  - Managing the overall effort, especially through Phase II development
- Integration Effort
  - Offerors support Navy in performing systems integration of vendor developed technologies

Typical Responsibilities

- Work with the team (e.g., government and award recipients) to …
  - Solidify requirements, interfaces…
    - Codify all "system level" requirements
      - Also address components, subsystems, etc.
  - Ensure OPNAV, Acquisition, user requirements are being addressed/met
  - Integrate selected technologies into overall system
  - Plan, schedule and conduct component, sub-system and system reviews
  - Schedule, coordinate and direct integration and testing events at the sub-system and system level

Critical Timeline

Event	Date	Time
Industry Day	24 February 2010	10:00am Eastern Daylight Time
White Paper Due Date	15 March 2010	2:00pm Eastern Daylight Time
Notification of White Paper Evaluation	11 April 2010	Close of Business
Full Proposal Due Date	21 May 2010	2:00pm Eastern Daylight Time
Notification of Selection: Full Proposals	4 June 2010	Close of Business
Awards	30 October 2010	Close of Business
These dates are estimates		

Questions

- Questions?
  - Open…
  - Written captured on form…

All questions will be captured in the FAQ

Break