ISSUES AND REQUIREMENTS FOR CYBERSECURITY IN NETWORK CENTRIC WARFARE

Martin R. Stytz, Ph.D.

WPAFB, OH
mstytz@att.net

Sheila B. Banks, Ph.D.
Calculated Insight
Orlando, FL
sbanks@calculated-insight.com

Introduction

- "The battlefield is the computer"

- The bad guys have many motivations for attacking computational resources
  - Psychological, military, and financial
  - Their advantage
  - Threat will increase
- Need to redress the balance

Motivation

- Network Centric Warfare (NCW) increases effectiveness by information-based empowerment
- Increased power from information leads to increasing reliance on information
  - Unspoken tenet of NCW is that information is accurate
  - The growing threat brings this assumption into question because information will be attacked
  - Growing sophistication and effectiveness of cyberbattlespace offensive activity
- Technical sophistication required to manage/conduct defense
- Increasing expertise offshore
- Increased vulnerability as software application size increases
  - Compounds the defensive problem

Motivation

- Current defenses are costly
  - Computationally
  - Financially
- Difficult to test current defenses
- Cyber security required across the entire cyberbattlespace
  - Networks, software, data
  - Broad variety of threats to each must be addressed
- Our goal
  - Understand and characterize the problem space
  - Foundation for work to redress the imbalance between defense and offense

Cyber Battlespace Arena - Scenario

- System launches multiple false attacks
  - Maximal havoc and confusion
- Under cover of false attacks, main attack thrust is unleashed
  - Stealthily penetrate network defenses
  - Aimed at a target software application
- When arrive at target application, obtain copy
- Rapidly analyze application, understand defenses, and penetrate target
- Make desired changes to target application
- Return target application to execute in place of original
- Back out of main attack thrust and gradually ramp down diversions

Cyber Battlespace Arena

- Events occur at high speed, much faster than human thought processes
- Rapid change in attack vectors
- Need for technical expertise for command and control
- Difficult to develop and maintain situation awareness
- Current lack of metrics to measure defense effectiveness
- Difficult to predict future activity in cyberbattlespace
  - No predictive battlespace awareness
- High degree of vulnerability to intended and unintended effects of cyberspace actions

Cyber Battlespace Background

- Traditionally have relied upon network and operating system defenses to protect software
- This dyad is not sufficient
  - Dyad does provide the basis for protecting software
  - Moving to triad
- Protection triad includes software protection
  - Protect decades of investment in high performance software and the research results they embody
  - Critical to every aspect of military activity, from training to operations
  - Protected software is the foundation for high confidence computing
  - All cyber attacks are, at their core, software attacks
    - This insight is the basis for our analysis and conclusions

Current Project Goals

- Address need for inherent cyber security
- Develop seamless web of protection
  - Extensible and responsive protection technologies
  - Protects all cyber resources
- Insure secure interoperation
- Provide inherent protection and inherent capability to determine if an application/resource is under attack or compromised
- First step - determine the attacks and document them
  - Learn the “terrain” of this new battlefield
  - Provide a framework for analysis to identify threats
- Result - Highly trusted data and applications that enable NCW paradigm

Attack Identification - Framework for Analysis

- Goals, effort, vector
- Goals of attacks
  - Reverse engineering all or parts of a code
  - Allowing limited or unrestricted execution
  - Tampering with the code
- Type of effort needed for successful attack
  - Human effort (from expert to ordinary skills)
  - Generic tools (COTS, open source)
  - Specialized tools (what is possible by skilled adversaries?)
  - Number of allowed executions
  - Time and availability of code required for attack
- Vector for attack
  - Specific vulnerability exploited; means for delivering attack payload

Attack Identification Methodology

- Identify each type of attack/exploit category
  - Web and literature survey
  - Narrative description
- Convert each narrative into UML threat case and sequence diagrams
  - Threat case diagrams to document threats; XML for annotations(s)
- Parallel development
  - Tests, scenarios, and experiments to validate uncovered attacks
- Testing and analysis of identified attacks and included major and minor threat cases
- Refinement
- Feedback

Attack Analysis Results - Overview

- No generally accepted classification
  - Developed classification based upon extensive research and correlation of literature
- Literature shows it is broad and growing
- Three basic attack strategies
  - Fault injection via environment
  - Fault injection through source
  - Fault injection via errors

Specific Attacks

1- Block Access to Libraries
2 - Redirect Access to Libraries
3 - Manipulate application registry values
4 - Force the application to use corrupt files or databases
5 - Manipulate and replace files that the application creates, reads, writes, or executes
6 - Force the application to operate in low memory, disk-space, and network-availability conditions
7 - Overflow input buffers
8 - Attack through application switches and options
9 - Use escape characters, different character sets, and commands to get malformed input
10 - Try common default and test names and passwords
11 - Look for and test unprotected application APIs
12 - Connect to all ports
13 - Fake the data source
14 - Create loop conditions in an application that reads script, code or other user supplied macros or logic
15 - Look for and use alternative execution routes through an application to accomplish its task(s)
16 - Force the application to reset its values
17 - Get between time of check of a value and time of use of a value
18 - Create fake files with the same name as protected files
19 - Force all error messages
20 - Look for temporary files for an application and examine their contents for sensitive or exploitable information
21 - Force invalid outputs to be generated
22 - Attack through shared data

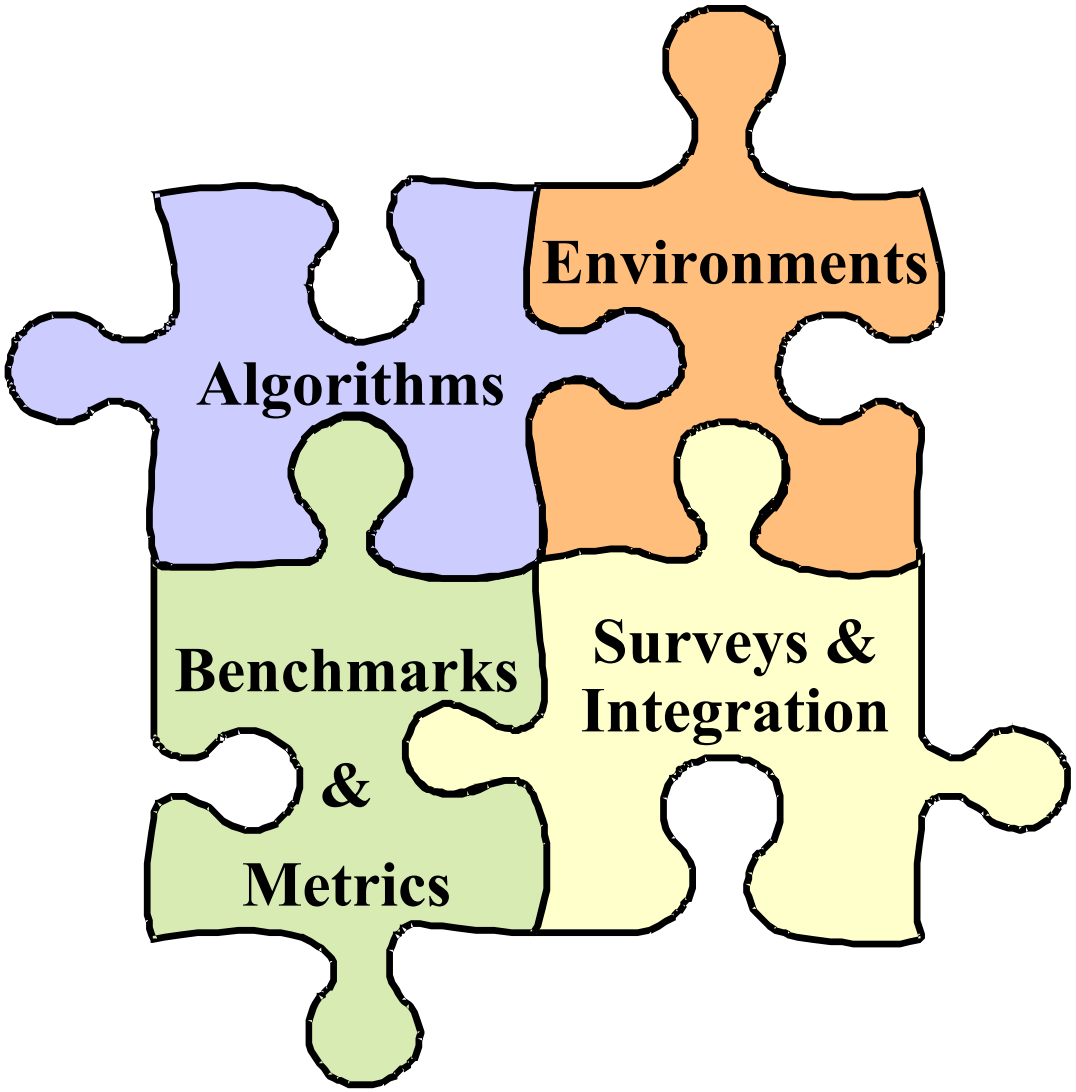
The Attacks - Requirements

- In light of the types of attacks, what response is necessary?
  - Preserve integrity/functionality of network
  - Control system use
  - Prevent extraction of software subsets (piracy)
  - Protect data
  - Protect network access
  - Insure correct and accurate software
  - Insure computations are correct and accurate
- Far from achieving these objectives
  - No methodology for development or maintenance
- Current strategies for defense are not effective
  - Separable
  - Not mutually supportive

A New Cyber Security Strategy

- Continue to apply defense in depth
- New philosophy for defense in depth
  - Paradigm that recognizes differences between physical and cyber worlds
  - Physical world makes defense in depth viable since attacks are sequential due to physicality
  - Cyber world has no counterpart
    - Independent and sequential attacks can occur in any order
    - Defeat defenses piecemeal
  - Defense in depth should be an interwoven set of defenses
    - Mutual support, mutually reinforcing, inseparable
    - Independent
    - Multiple simultaneous challenges

Research Requirements



Additional Requirements

- Implement new cyber defense in depth
- Benchmarks, metrics, and test suites
  - Autonomous cyber red team
- Ontology and lexicon
- Black box application of protection technologies
- Cross authentication of components
- Autonomous, secure assembly and verification of security capabilities
  - Truly composable protection techniques
- Data protection
- Inherently secure programming languages
- Process to maintain secure software

Conclusions

- The transition to NCW brings with it an increased imperative for secure, trustworthy data
- Current capabilities do not address the challenge
  - New cyber defense strategy and research requirements
  - Need for NCW cyber security discipline
- Wide variety of attacks to be addressed
- Need to employ and devise new techniques for network, software, and data protection against attacks
  - New strategy
  - Several development needs

Conclusions (cont.)

- Need ability to test and evaluate defenses
- Need to measure effectiveness of defenses
- Need new approach for software development from requirements to maintenance
  - Entire lifecycle
- Need integral cyber security
  - Present in all software, network systems, data
  - Designed in and not patched on
- Need science of cyber protection
  - Especially as related to NCW

Summary

- "The battlefield is the computer"

- NCW makes software, networks, and data ever more tempting targets
- Wide variety of attacks to be addressed
  - Currently increasingly effective and sophisticated
- Need to accelerate development of defensive technologies to change the protection balance of power