TOWARD USING INTELLIGENT AGENTS TO DETECT, ASSESS, AND COUNTER CYBERATTACKS IN A NETWORK-CENTRIC ENVIRONMENT

Martin R. Stytz, Ph.D.       Dale E. Lichtblau, Ph.D.       Sheila B. Banks, Ph.D.
Institute for Defense Analyses, Washington, DC  Institute for Defense Analyses, Washington, DC  Calculated Insight, Orlando, FL
mstytz@ida.org
mstytz@att.net
del@ida.org
sbanks@calculated-insight.com
Introduction

- “The battlefield is the computer”

- The bad guys have many motivations for attacking computational resources
  - Psychological, military, and financial

- Threat will increase

- So, our primary NCO resource is also a prime target
Introduction (cont.)

- 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
- State and security of network will be critical to commanders
- Speed and complexity of cyberspace indicate that new defense approaches are needed
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 serendipitous effects of cyberspace actions
In light of the types of attacks, what response should be made?

- 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

Resultant CGF Capability Needs

- Architecture
- Distributed system (scale)
- Knowledge acquisition
- Cyber sensors
- Most important task is knowledge acquisition for defense management
Framework for Analysis of Attack

- **Goals, effort, vector**
  - CGFs must be aware of all three

- **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

- Parallel development
  - Tests, scenarios, and experiments to validate uncovered attacks

- Testing and analysis of identified attacks and included major and minor threat cases
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
Types of 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 tasks
16- Force the application to reset its values
17- Get between time of check of a value and time of use of 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 output to be generated
22- Attack through shared data
Basic Research Requirements

- Algorithms
- Environments
- Benchmarks & Metrics
- Surveys & Integration
CGF Cybersensor Requirements

- Data acquisition about local attack
- Identify type of attack, attack payload, strategy
- Attack origination
- Must be able to identify an attack and differentiate it from a system failure or fault
- Secure transmission of data from sensor to control sensor
- Secure migration
- Autonomic operation
- Exchange data among cybersensors securely
- Scan for vulnerabilities and assess risk
Addressing the Need

- Must develop techniques and environments to assemble the CGF cybersensorss
- Must test the CGFs as well
  - Real world too dangerous
  - Simulation environments provide protection for real-world and required complexity for CGF testing
- Develop application security test suites
- Build testbed for development and evaluation of technologies and CGFs
  - Secure development
  - Benchmarks, metrics, scenarios
  - Integrated cyber defensive techniques for testing and analysis
  - Techniques for testing of methodologies
- Need cost-benefit analysis for different types of security
Conclusions and Future Work

- Transition to NCW will place a premium on cybersecurity
- Speed of activity in cyberspace calls for automated defenses
- CGFs will have many functions to perform and much remains to be done before they can be fielded
  - Identified requirements and attacks they must be able to manage
- Need to refine requirements and develop distributed CGF system