NetCentric Technology, Inc.

# Army Battle Command Systems (ABCS) Security Testing: A Systems-of-Systems Approach

Sam Nitzberg and John Skrletts

MILCOM 2005

NetCentric Technology, Inc.

# Introduction

Successful approach to perform security systems-of-systems testing – used for security testing of tactical systems

Identifies:

- Operational benefits of implemented security architectures and models,
- Intrinsic security strengths and weaknesses of security devices used, and
- How networks of interacting systems behave in real attack-and-defend scenarios

NetCentric Technology, Inc.

# White Box Testing

Provides detailed insights at the component-level.

REQUIRES: Possession and understanding of system,code,and design internals

HOWEVER: Requires significant post-analysis risk assessment

NetCentric Technology, Inc.

# Black Box Testing

Identifies functional component behavior

REQUIRES: Well-defined and understood component behavior

HOWEVER: Comprehensive Black Box Testing is difficult to achieve

NetCentric Technology, Inc.

# Systems-of-Systems Testing

Provides tangible analysis of expected performance in networked and internetworked environments

Identifies true vulnerabilities – not susceptibilities.

Identifies vulnerabilities due to architectural dependencies

REQUIRES: Architecture representative of security-relevant fielded network/s and deployed environments, given a stated test objective.

HOWEVER: Requires methodical approach and organizational support

NetCentric Technology, Inc.

# SOST Test Objectives

Choose a focus of the SOST:

- Network – based Assessments
- Interaction of systems on network
- Applications security analysis
- IA Management systems
- Other…

NetCentric Technology, Inc.

# Key Steps

1) Identify relevant targets (systems,software,hardware)
2) Design testbed
3) Plan tests
4) Establish appropriate teams
5) Build test floor
6) Conduct tests
7) Review results; Evaluate results and take appropriate actions

NetCentric Technology, Inc.

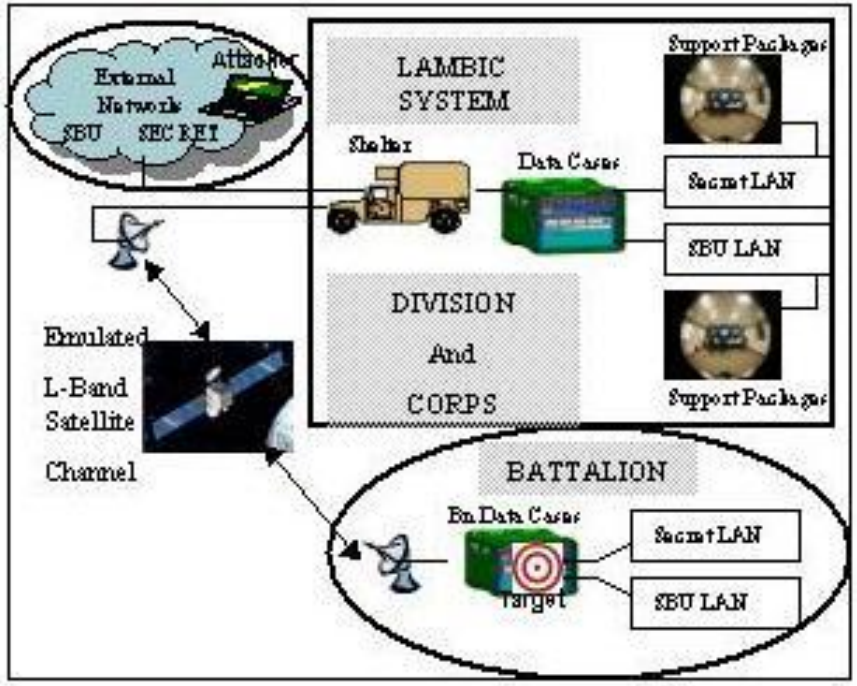
# Typical Test Case Types

- Authentication / Authorization
- Denial-of-Service
- Specialty cases

NetCentric Technology, Inc.

# Example Test Case

| | |
|---|---|
| Objective: | Undermine Router Security |
| Type: | Authentication / Authorization |
| Source: | External Networks |
| Target: | Router in data case |
| Description: | Attack will be against router IOS |
| Procedure: | Conventional attacks to falsely authenticate to router. |
| Red Team: | Perform attacks |
| White Team: | Monitor and preserve logs<br>Record results |




For each specific test case, an objective, source of attack, target location, a brief description of the attack to be performed, and a procedure to use to perform the test is indicated. Actions taken by teams are also denoted.

NetCentric Technology, Inc.

# Conclusions and Experiences

SOST Testing is reliable, repeatable, and cost-effective.

SOST Testing can provide real-world results without necessitating a live or production environment

SOST Testing can validate effective aspects of security architectures, and reveal hidden flaws

# Contact Information

John Skrletts / Sam Nitzberg

NetCentric Technology, Inc.

(732) 544-0888

http://www.netcentricinc.com

jskrletts@netcentricinc.com

snitzberg@netcentricinc.com