Defense Advanced Research Projects Agency
Information Assurance and Survivability
Operational Experimentation (OPX)

Phoenix Challenge 2002

Brian Witten
OPX Program Manager
bwitten@darpa.mil
Information Assurance and Survivability Operational Experimentation (OPX)

Witten, Brian

DARPA

DISTRIBUTION/AVAILABILITY STATEMENT
APUBLIC RELEASE

15. SUBJECT TERMS
IATAC Collection

19b. TELEPHONE NUMBER
International Area Code
703767-9007
DSN
427-9007

See report.

See report.
**Information Assurance and Survivability Operational Experimentation (OPX)**

Witten, Brian

DARPA

Defense Advanced Projects Research Agency

This briefing was presented during the Phoenix Challenge 2002 Conference and Warfighter Day.
Vision

- New Capability: Situational Awareness
- Reduce Overload: Analyst Workbench
- Protect Centers of Gravity: Survivable Servers
- Pervasive Sensors: Hardened Clients
Objectives:
- Accelerate transition of effective technologies
- Inform research agenda with operational experience

Key Experimentation Risks, Transition Metrics:
- Limited operational staff time
- Impact on operational systems

Approach:
- Leverage mature research, well tested in lab
- Field cautiously: walk before we run
The Analyst’s Challenge

Impact of Transition to T3 volume at Internet Access Points

Potential IAP Traffic (T3)

Today

Tomorrow
Intrusion Detection in the Lab

**DARPA 1998 Results (MIT/LL and AFRL)**

- **Operational sensors:**
  - Hundreds of false alarms per attack
  - Actually miss most attacks

- **Research sensors:**
  - Dramatically reduce false alarm rates
  - Substantially improve detection coverage
Analyst Workbench

- Analysts currently overwhelmed
  - Flood of data, high false alarm, low detection rates
  - Not... real time, decision quality, always actionable

- DARPA Algorithms
  - Over a dozen lab tested real time algorithms
  - Data mining, anomaly, self organizing, expert systems

- Execution: September 2001 – September 2002
Hardened Client

- MARFORPAC Challenge
  - Classic SIPR/NIPR PC problem
  - Compounded by TAD laptop theft
  - Insider threat and unknown viruses

- Proposed Technology
  - Safe e-mail “wrappers” and encrypting file system
  - Autonomic Distributed Firewall
  - PGP Disk & Disk Eraser
Operating System Wrappers

- Trap and stop unknown viruses
- Enable safer use of mobile code
- Performance impact: Low
- Availability: Solaris, Linux, NT, Win2K

Developers: Network Associates, Teknowledge, Cigital, Telcordia
Autonomic Distributed Firewall

- Firewall on Network Interface Card (NIC)
- Hardware based cryptographic accelerator
- Trustworthy control of untrustworthy OS

**ADF Controller**
- Converts high level policy into low level packet filtering rules for each NIC
- Triple redundancy, manages thousands
- Drag and drop INFOCON changes
- Encrypted communication with NIC
- Audit database and browser

LAN → NIC → Workstation
LAN → NIC → Server
NIC → Internet → Remote user

Made by Secure Computing and 3Com
Research performed under DARPA sponsorship
Hardened Client Timeline

- MARFORPAC Limited Objective Experiment
  - Apply safe e-mail wrappers and encrypting file system
  - MARFORPAC approved internal experiment charter
  - Execution: Late CY2001, RSO&I 02, UFL 02

- Fleet Battle Experiment India (C3F)
  - Execution: Jun 2001 – Autonomic Distributed Firewall (PCI)

- Fleet Battle Experiment Juliet Goals (PACFLT)
  - Complete application of diverse wrappers
  - Autonomic Distributed Firewall (PCMCIA)
Motivating factors:
- High-value and commonly targeted center of gravity
- Need Intrusion Tolerant Systems:
  *Ability to confidently execute mission while under attack*
- Reactive defense not adequate

Possible technologies:
- PASIS: Perpetually Available Survivable Information System
  *Leverage fragmentation, redundancy, and scattering*
- SELinux, Immunix, Emerald, NetTop Vmware, Wrappers

Execution: 2002
Situational Awareness

- Am I under attack?
- What is the nature of the attack?
  - Class, mechanism, and source
- What is mission impact?
  - Urgency, damage assessment and control, initial response
- When did attack start?
  - More detailed damage assessment. What have I done wrong?
- Who is attacking?
  - What are they trying to do? What is their next step?
- What can I do about it?
  - Course of action analysis, collateral damage risk, reversibility
Theater C4I Coordination Center
PACOM TCCC

**Need**
- Theater Wide
- Real Time
- Decision Quality
- Actionable Information

**Strategy**
- Leverage Cyber Panel emerging research

**Network Management**

**Information Dissemination Management**

**Information Assurance**
Summary

FY 01
- Analyst’s Workbench
  - PAC CERT
- Hardened Client - MARFORPAC, PACFLT

FY 02
- Possible extension to other CERTS
- Survivable Server
- Situational Awareness - TCCC
Context

- Functionality
- Performance
- Security
- Availability
- Confidentiality
- Integrity

Tolerance Detection Prevention

Layered Protection Dynamic Defense

Attacks

Risk-Balanced Optimizing Strategy

Information Treasures

Methodology