AFRL Defensive IO Programs

William E Wolf
AFRL/IFGB
525 Brooks Road
Rome NY 13441
wolfw@rl.af.mil

Lt Col Richard Simpson
AFRL/HEX
2255 H St. Bldg 248
WPAF Ohio 45433
Richard.Simpson@wpafb.af.mil
**AFRL Defensive IO Programs**

**Unclassified**

**Performing Organization Name and Address**
AFRL/IFGB
525 Brooks Road
Rome, NY 13441

**Performing Organization Report Number**

**Sponsoring/Monitoring Agency Name and Address**
USAF

**DISTRIBUTION/AVAILABILITY STATEMENT**
PUBLIC RELEASE

**Supplementary Notes**
See report.

**ABSTRACT**
See report.

**Subject Terms**
IATAC Collection

**Security Classification of:**

- **REPORT**: Unclassified
- **ABSTRACT**: Unclassified
- **THIS PAGE**: Unclassified

**Limitation of Abstract**
Public Release

**Number of Pages**
17

**Name of Responsible Person**
Email from Booz, Allen, & Hamilton (IATAC),
fenster@dtic.mil

**Telephone Number**
International Area Code
Area Code Telephone Number
703-767-9007
DSN
427-9007
<table>
<thead>
<tr>
<th>1. AGENCY USE ONLY (Leave blank)</th>
<th>2. REPORT DATE</th>
<th>3. REPORT TYPE AND DATES COVERED</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>4. TITLE AND SUBTITLE</th>
<th>5. FUNDING NUMBERS</th>
</tr>
</thead>
<tbody>
<tr>
<td>AFRL Defensive IO Programs</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>6. AUTHOR(S)</th>
<th>7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)</th>
</tr>
</thead>
</table>
| Wolf, William E.; Simpson, Lt. Col Richard | Air Force Research Laboratory  
525 Brooks Rd.  
Rome, NY 13441 |

<table>
<thead>
<tr>
<th>8. PERFORMING ORGANIZATION REPORT NUMBER</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)</th>
<th>10. SPONSORING / MONITORING AGENCY REPORT NUMBER</th>
</tr>
</thead>
</table>
| Air Force Research Laboratory                             | Air Force Research Laboratory  
525 Brooks Road, Rome NY 13441 |

<table>
<thead>
<tr>
<th>11. SUPPLEMENTARY NOTES</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>12a. DISTRIBUTION / AVAILABILITY STATEMENT</th>
<th>12b. DISTRIBUTION CODE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Approved for public release; Distribution unlimited</td>
<td>A</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>13. ABSTRACT (Maximum 200 Words)</th>
</tr>
</thead>
<tbody>
<tr>
<td>This briefing on Defense IO Programs was presented during the Phoenix Challenge 2002 Conference &amp; Warfighter Day.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>14. SUBJECT TERMS</th>
<th>15. NUMBER OF PAGES</th>
<th>16. PRICE CODE</th>
</tr>
</thead>
<tbody>
<tr>
<td>IATAC Collection, information operations, Cyber Wolf</td>
<td>16</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>17. SECURITY CLASSIFICATION OF REPORT</th>
<th>18. SECURITY CLASSIFICATION OF THIS PAGE</th>
<th>19. SECURITY CLASSIFICATION OF ABSTRACT</th>
<th>20. LIMITATION OF ABSTRACT</th>
</tr>
</thead>
<tbody>
<tr>
<td>UNCLASSIFIED</td>
<td>UNCLASSIFIED</td>
<td>UNCLASSIFIED</td>
<td>UNLIMITED</td>
</tr>
</tbody>
</table>
Information Assurance

• **Definition**
  – Information operations that defend the global information enterprise through employment of Protect, Detect, Assess and Respond capabilities. This is accomplished by ensuring availability, integrity, authentication, confidentiality, and non-repudiation (based on DODD S-3600.1 & AFDD 2-5).

• **Approach**
  – Develop technology for and transition technology to AF, DoD and National customers
  – Continuous capability improvement through experimentation with warfighter, spiral development, leverage of COTS, and technology transition, e.g., CAOC-X, JBI, etc...

• **Value to the Warfighter**
  – Accurate, trusted, reliable warfighter information
  – Survivable information systems and networks
  – Information superiority through assured information operations
Information Assurance
“A Short History”

• **Pre 1970’s**
  – Encryption

• **1970’s**
  – Computer Security R&D begins (“Test and Patch”)

• **1980’s**
  – Multilevel Security
  – Strong Security Based on Special-Purpose Systems
  – Risk Avoidance
  – “Orange Book” Evaluation Criteria

• **1990’s**
  – Movement Towards COTS Software
  – Perfect Security Recognized as Unachievable
  – Risk Management

• **2000 & Beyond**
  – Trend toward Information Survivability
  – Situational Awareness
  – Intrusion Tolerance
  – Active Response
Information Assurance
Today’s Capability

Protect
– Encryption (VPN, Digital Signature, PKI, etc.)
– Firewalls/Guards/Boundary Controllers
– Passwords, Biometrics
– Trusted Operating Systems/Database Management Systems
– Physical Security (Stovepipes, Vaults, etc.)
– Vulnerability Scanners
– “Penetrate and Patch”

Detect
– Virus Scanners (Signature-Based)
– Intrusion-Detection (Signature-Based)
– Auditing

• Assess
  – Computer Forensics Tools (Media Imaging, Data Recovery, etc.)
  – CERT’s

• Respond
  – Physical Media Relocation
  – Backups
Vision

• Protect the GIE with a high degree of confidence
  – Assured defense-in-depth against a wide variety of threats
  – Understand/manage risks and plan for protection
• Detect information attacks
  – Early warning using light weight cooperating sensors
  – Efficient, accurate data reduction, fusion, correlation
• Assess information attacks
  – Identify adversary, nature, timing, severity
  – Determine mission impact
  – Develop courses-of-action
• Respond to a successful IW attack in an appropriate manner
  – Graceful degradation, recovery, reconstitution
  – Feedback to improve protection and detection processes
  – Offensive Information Operations
Information Assurance Vision

Attacks, Malicious Code, ...

Attacker

Restored

Tolerant

Inoperable

Respond → Assess → Detect → Protect

Knowledge Base

Global Information Grid

Active Response (Traceback, Fingerprint, ID)
National Scale INFOSEC Hard Problems
[By the INFOSEC Research Council]

• Intrusion/Misuse Detection & Response
• Foreign & Mobile Code
• Controlled Sharing of Sensitive Information
• Application Security
• Denial-of-Service
• Communications Security
• Security Management Infrastructure
• Security in Mobile Environments
• Security Engineering Methodologies
• Influencing Vendors
Technical Approach

High Assurance
RF Protect
Secure Mobile Code
Boundary Controllers
Embedded Systems IA
Wrappers

Intrusion Tolerance
Active Response
Fault Tolerant Networks
Effects-Based IO
Assured QoS

Situation Awareness
Forensics
Decision Support & IO Planning

Early Warning
Data Hiding
Sovereign Time

Data Mining
Intelligent Agents
Auto Intrusion Detection Env
AF Enterprise Defense
Wireless Intrusion Detection

Full Spectrum IA

Protect
Respond
Assess
Detect
Success Stories

- DAIWatch
- CYBERWOLF
- Wireless Information Assurance
- Steganography
- Air Force Enterprise Defense (AFED)
Objective: Enhance level of Information Assurance by utilizing breakthroughs in software agent and fusion technologies that provide revolutionary flexibility, extensibility, and reliability

Approach:
- Agent Technology via Java Aglets
- Dynamic distribution of multiple host sensors
- Integrated multi-dimension graphical analysis

DAIWatch Revolution
- Finds the most sophisticated attackers
- Reduces security administration
- Adjusts to risk and minimizes overhead
- Not vulnerable to compromise

Technology Transition
- Phase III SBIR
- AFIWC – agreements to integrate DAIWatch with CIDDS
- JBC – DAIWatch selected for operational demonstration (focused on ability to transport functions and data across SIPRnet)
- Beta Test Program with a commercial investment company
**Problem:** Network Defenders cannot process thousands of low level events in real time.

**Objective:** Enhance network defense by automatically correlating network management events with Intrusion Detection System (IDS) events to provide accurate situational information.

**Approach:**
- Place lightweight device experts on all network assets
- Device experts adaptable to specific installations operational security policy
- Remotely manage geographically separate installations in a 24/7 mode

**Technical Challenges**
- Distribute event processing between enterprise and device
- Design and implement device experts for all types of network assets
- Encapsulate Net defenders knowledge into Rule structure
- Reduce 1000’s of net events to a few highly reliable incidents

**Status**
- Cyberwolf correlating events from AFRL RRS NOC
- Cyberwolf commercialization effort fully underway with several potential customers
- Correlation capability from Cyberwolf is being channeled into AFED program
- Rule set currently exceeding 2000 entries
- Cyberwolf under evaluation for use by several large corp. and a Canadian bank for network enterprise protection

**CyberWolf Architecture**

**Tech Transitions**
- Federal Emergency Management Agency
- Naval Sea Systems Command
- Air Force Research Lab
- Joint Battle Center
- Land Information Warfare Activity
**Objective:** Enhance and extend IA for wireless through synergistic in-house and contractual activities

**Current Projects:**
- Wireless Intrusion Detection & Distributed Boundary Control
- Combined Access Point/Firewall/VPN/Intrusion Sensor Device
- Wireless & Mobile Authentication/Key Revocation
- Adaptive RF Wireless Nodes
- Software Defined Radio for Wireless Information Assurance
- Intrusion Detection Agents for Handheld Devices
- Automated Wireless LAN Compliance Monitoring Techniques
- AF Wireless Security Architecture Development
- DOD Overarching Wireless Policy Development

**Accomplishments:**
- Developed site survey and compliance monitoring techniques
- Created wireless architecture adopted by AF
- Developed and demonstrated wireless intrusion detection and policy violation detection techniques
- Provided key inputs to DOD overarching policy
- Assessed netstumbler.com threat in the context of AF base locations

**Wireless IA Problem Space:**

- Protect
- Detect
- Respond

- Application
- Presentation
- Session
- Transport
- Network
- Data link
- Physical

Wireless Emphasis
Smart Digital Data

Technology Area Payoff

- Information Assurance
  - data & source authentication
  - tamper detection & data recovery
  - automatic data dissemination through guards; classification & license marking
  - detection & identification of adversary steganographic activity & extraction of hidden data
  - tracing sources of data leaks
  - minimize data loss (corrupt data pointers; invalid data headers)

- Information Enhancement
  - embedded auxiliary information (images, documents, overlays, audio, links, etc.)
  - multi-level data release to coalition forces; key-based access
  - covert communication
  - maximize throughput of communication channels
**Air Force Enterprise Defense**  
**AFED**

### Infrastructure

![Infrastructure Diagram]

### Objectives
- Provide a **Defense-in-Depth** capability that integrates existing event information:
  - Policy Enforcement; Change/Configuration Management; Threat & Vulnerability Assessment with Countermeasure recommendations; Intrusion Detection; Network Management
- **Fuse** Information Assurance (IA) and Network Management data into a **Common Enterprise Picture**
- Provide a consistent visual environment for information portrayal

### Approach
- Spiral tech exploration, development, validation, and feedback process
  - Automated Reporting for Containment and IO Targeting
  - Mission Situational Assessment
  - Automated Courses of Action

### Payoffs
- Integrates existing enterprise sensors and provides enhanced Information Assurance and Enterprise Defense capabilities in support of the AF Protect-Detect-React/Restore model.
- Assists in the automated detection and reporting of information attacks, containment and restoration of compromised systems, and planning/protection of enterprise assets.
- Supports entire NOSC mission by cross-sharing of data among NOSC crew

### Transition Agents:
ESC/DIGC, ESC/DIW

### End Users:
MAJCOM NOSCs, AFNOSC, CAOC-x
Vision

• “NOSC-in-a-box”—one application integrates all NOSC tools

• One application addresses needs of entire NOSC crew
Summary

• The AFRL/IF program includes all aspects of the IA problem
  – Protect
  – Detect
  – Assess
  – Respond

• Addressing the hard IA problems
  – Leading edge technology

• Addressing technology at all levels
  – Basic Research
  – Exploratory Development
  – Advanced Development