AFCEA Panel: Techniques for Information Assurance

Network Security Improvement Program

Michael L. Gentry, Ph.D.

17 Sep 98
<table>
<thead>
<tr>
<th>Report Date</th>
<th>Report Type</th>
<th>Dates Covered (from... to)</th>
</tr>
</thead>
<tbody>
<tr>
<td>(&quot;DD MON YYY&quot;)</td>
<td>N/A</td>
<td>(&quot;DD MON YYY&quot;)</td>
</tr>
<tr>
<td>17091998</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Title and Subtitle</th>
<th>Contract or Grant Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>AFCEA Panel: Techniques for Information Assurance Network Security Improvement Program Program</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Authors</th>
<th>Project Number</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Performing Organization Name(s) and Address(es)</th>
<th>Performing Organization Number(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Army Signal Command</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Sponsoring/Monitoring Agency Name(s) and Address(es)</th>
<th>Monitoring Agency Acronym</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Distribution/Availability Statement</th>
<th>Monitoring Agency Report Number(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Approved for public release, distribution unlimited</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Supplementary Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Abstract</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Subject Terms</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Document Classification</th>
<th>Classification of SF298</th>
</tr>
</thead>
<tbody>
<tr>
<td>unclassified</td>
<td>unclassified</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Classification of Abstract</th>
<th>Limitation of Abstract</th>
</tr>
</thead>
<tbody>
<tr>
<td>unclassified</td>
<td>unlimited</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Number of Pages</th>
</tr>
</thead>
<tbody>
<tr>
<td>20</td>
</tr>
</tbody>
</table>
# AFCEA Panel: Techniques for Information Assurance

**Author(s):** Michael L. Gentry, Ph.D.

**Performing Organization:**
IATAC
Information Assurance Technology Analysis Center
3190 Fairview Park Drive
Falls Church VA 22042

**Sponsoring Agency:**
Defense Technical Information Center (DTIC-IA)
8725 John J. Kingman Rd, Suite 944
Ft. Belvoir, VA 22060

**Abstract:**
This AFCEA briefing outlines a construct for Techniques for improving information assurance and network security. The security plan is outlined in phases that build the foundation, harden the infrastructure and then insert new technology. The program relies on defense in depth and involves all Army Major Commands (MACOM).

**Subject Terms:**
Network security, information assurance, afcea
Network Security Improvement Pgm

**Phase I**
- Workstation and Server-based security
- ID and Passwords
- TCP Wrapper
- Security Scanning
- Anti-Virus

**Phase II**
- Intrusion Detection System Reporting to DOIM and CERTs
- Router-Based Security (Filtering)

**Phase III**
- Install Firewalls (If Needed For Specific Network Security Rqmts
- One-Time Passwords

---

**Build Foundation**

**Harden Infrastructure**

**Insert New Technology**
C2 Protect VCSA Direction

"...Implement Near-Real-Time (NRT), worldwide, common picture of the Army’s Military Information Environment (MIE)

...Combine the Army’s Information Service Provider functions with Army Regional Computer Emergency Response Team (RCERT) C2 Protect/ISS services

...Ensure reporting of a common picture of the Army MIE to a central coordination center

...Enhance acquisition of unified and global NRT protect, detect, and react capabilities through physical integration of functions and virtual collocation at Network & Systems Operation Centers and Regional Computer Emergency Response Teams....."
Focus of Operation INFO GUARD

- Establish a Hasty Defense for the Sustaining Base information system environment
  - Establish intrusion detection on Army NIPRNET connections
  - Establish intrusion detection on limited set of high profile Army servers
  - Establish a global view of the Army NIPRNET and SIPRNET connectivity
  - Establish a protected Army Domain Name Service (DNS) system
  - Implement basic configuration management and control capabilities

- Prepare plans for a deliberate Defense in Depth starting FY99
The Army Signal Command

24x7 Operational Forward Presence

ASC
- Networks Operation, Monitor, & Restore
- Systems Operation, Monitor, & Restore
- Integrated C2 Protect
- Global Configuration Control

LIWA
- Analysis
- Info Dissemination
- Coordination/Reporting
- Computer Defense Assessment Program
- Database Tools
- Attack & Response

Coordination & Reporting
World Wide Network View
NSOC = Network and Systems Operations Center
RCERT: Regional Computer Emergency Response Team
Organizational Concept of Operation
(Unified CINC Perspective)

CINCEUR

Global Operational and Planning Presence with CINCs

The Army Signal Command
Basic Security Architecture

External Network

IDS

Security Router
* Packet Filtering
* Some SNMP Trapping
* Basic Anti-Spoofing

Ether Switch

DMZ

Public
* Public Policy Enforcement

Web Server*
* Host Based Security

DNS Server*

* Added Layer of Security
* Tighter Anti-Spoofing

Interior Router
* Private Policy Enforcement

Private

Users

Web
FTP
Org DNS
Worldwide Network View

- **IOC**: 15 July
  - Near Real Time view of CONUS and Europe NIPRNET

- **FOC**: 28 October
  - Near Real Time view of NIPRNET worldwide
  - Near Real Time view of SIPRNET worldwide

DATA IS CURRENT WITHIN 5-15 MINUTES
Centralize Management and Configuration Control

- **IOC:** 30 September
  - Centralized Access Control List Management of security router
- **FOC:** 27 November
  - Router configuration management
  - Configuration control of IDS engines & DNS servers
  - Configuration control Golden Master established
  - Configuration control board staffed with engineering support
CND R&D Thrusts
3 Main Areas

- Policy-driven Intelligent Agents for monitoring/analysis of high volume event flows
- Improved Data Visualization techniques for more intuitive situational awareness
- Improved sensor technologies for monitoring high-speed data flows
GUI based "Policy Manager" allows systems operators to establish management 'Policies' which are translated to "rules" for execution by Intelligent Agent objects.

Intelligent Agents - Software Objects driven by rule-based continuously monitor the CIM and execute domain specific controls based on pre-defined rules.

Common Information Management Environment - Object Oriented Framework provides a convergence of event information from a multitude of sensors within the enterprise into a single event store (database).
Current data visualization techniques are either tabular event tables or simple graphs depicting topology relationships between objects. Some objects are physical devices, others are logical constructs such as user accounts or databases. Relationships between these objects are not easily discernible with current display technologies.

NOC Operators are being flooded with hundreds of thousands of events occurring on thousands of objects. Current data visualization capabilities will not scale to the enormous flow of information that needs to be analyzed. More intuitive data visualization techniques are going to be essential to communicate true situational awareness and appropriate defensive responses.
Current IDS sensor technologies are not capable of operating effectively at available wire speeds such as ATM or Gigabit Ethernet. As backbone network speeds continue to increase to nearly back-plane speeds, the current IDS technologies threaten to become unacceptable bottle-necks on the information highway. New technologies for improving security sensing capabilities have got to be developed.
Network Security Improvement Pgm

Phase I
- Workstation and Server-based security
- ID and Passwords
- TCP Wrapper
- Security Scanning
- Anti-Virus

Phase II
- Intrusion Detection System Reporting to DOIM and CERTs
- Router-Based Security (Filtering)

Phase III
- Install Firewalls (If Needed For Specific Network Security Rqmts
- One-Time Passwords

Build Foundation

Harden Infrastructure

Insert New Technology
C2 Protect

Conclusion

Army’s initial C2P security architecture *in place*

Standardized systems architecture *critical*

Continuous effort required to improve our security posture