Interactive Visualization Development For Rapid Response

Therese Metcalf

October 2006

Approved for Public Release; Distribution Unlimited - 06-1271
Overview - Modified Systems Development Approach

- Accelerated system engineering process presented through an example development effort
Concept – Problem/Solution

Problem: No global view of Computer Network Defense (CND) status – Results in limited data for decision making and lack of integrated defense tactics

- Limited data presentation integration
- Fragmented situational awareness
- Need for overall understanding
- Lack of global visualization

Solution: Interactive three-dimensional (3D) Graphical User Interface (GUI) display presenting a fusion of actual NetD attack status in real-time across the cyber domain, enhancing user perception of dense defensive Information Warfare (IW) data for situational awareness, quick assessment, decision-making, and immediate response to experienced threat activity.

Current data is disparate and presented in a tabular format limits quick assessment.

Differing products present their unique, but restricted view of the global situation.

Basic Data (Data Points)
- Information (integrated display)
- Knowledge (layered Information)
- Understanding (scenarios)
- Decision Making (response)

Capabilities not available in Commercial-Off-The-Shelf (COTS) software

“The [display] requirement has been around since day one of the mission inception.
Requirements - Tracking

- #: Requirement tracking number
- Requirements: A brief description
  - White: Open Requirements
  - Gray: No longer relevant, OBE
  - Blue: Details TBD, Priority 5
  - Green: Implemented & Tested
- Suggestion: description of enhancement provided by a user –
- Modules: Requirement applied to
- Related Modules: Potential module(s) effected
- Priority: Original & New Priority
  - 1: Immediate, next release
  - 2: Following release
  - 3: Will be completed in designated timeframe if enough resources
  - 4: Will investigate possibility
  - 5: Will consider in the future
  - D: Delivered in operational prototype
- Source: Requirement submitter
  - UD: User Derived Requirement
  - DD: Developer Derived Requirement, may be suggestions from the field or the Display team
- Status Type: The status of the suggested enhancement
  - Reviewed: By Display Team, disposition indicated
  - Evaluation: Under evaluation by Display Team
  - Pending: Evaluation by Display Team
- Disposition:
- Release: Version requirement will be included within
- Questions/Comments
- Query: Query tool required
- Wks: Weeks to work
User Derived Needs

- First glance should tell overall health and what’s up and what’s down (i.e., core services)
- Want as much information presented as possible (i.e., aggregation) on one screen
- Global display that provides a status of alerts and sensor status
- Pull data and consolidate relevant facts into an integrated display (i.e., provides summary information by layer – e.g., TCP/IP model)
- Drill down for additional information

- Accurate and timely, to include IW and general status notifications
- Easy on the eyes (i.e., salience)
- Standardized views
- Easy to use (i.e., intuitive - not much training needed, people are changing all the time)
Community Requirements

Primarily
- Situational Awareness/Common Operational Picture (COP)
- Dynamic Performance Monitoring
- Ability to centrally monitor and collect configuration information
- Need visualization tools for analyst, operator, and decision support and effective indications and warnings

Secondarily - Related
- Computer Network Defense (CND) Concept Exploration
- Dynamic Mapping of Systems and Connections
- Need to provide commander with positive control of information resources
- Need to prioritize and dynamically allocate access
- Need ability to centrally manage security posture of enterprise applications and equipment

Other Efforts
- Present different views of managed objects on the display to meet the need of users
- Provide multiple level drill-down capabilities (additional linkages to be established between modules in the future for
- Provide the capability of launching element managers and other network/system managers for a physical object
- Present information associated with the managed objects including object dependency data
Human Machine Interface (HMI) Factors

- **User Interface**: Specification of a conversation between the user and the computer
  - GUI
  - Display
  - Zones
  - Messaging
  - Dialogue Tone and Terminology
  - Function Keys
  - Color Selection

- **Reporting**: Major output functionality, accuracy and clarity are fundamental, focus on formatting and generation

- **System Functionality**: Applicability of functions, data capture and format, processing capabilities, and system support to retain usefulness
  - Usability
  - Processing
  - System Errors
  - Data
  - Audio Outputs
  - Maintenance

- **Support Documentation & Training**: Proper and effective use, complete routine and unique tasks, and troubleshoot problems
  - System Documentation
  - Training and Training Material
HMI Considerations

User should expect:
- To be aware of what to do next
- To know system expectation
- Data checking--has been entered correctly or not
- Explanation of delays
- Task completion notification
- Standardized formatting, information, instructions
- Messages appear in the same general area and remain long enough to ‘read’ them
- Dialogue be limited to one idea per frame, whether paging or scrolling through the zone

Criteria:
- Ease of use
- Human Factors Engineering
- Documentation
- Training
- Security
- Maintainability
- Reliability
- Interoperability
Operational Platform Requirements

- Best viewed on a large screen display (Note: plasma screens have burn in issues)
- High-end graphics card:
  - ATI Radeon
  - Visiontek NVIDIA GeForce
  - Appian Jeronimo Graphics Card

- Personal Computer (PC) based systems
  - Desktops (e.g., Dell Dimension)
  - Laptops (e.g., Dell Inspiron)

- Windows Operating Systems (OSs)
  - XP (Experience)
  - Windows 2000
  - NT (New Technology)
Identify related components and needed integration
  – Conflicts
  – Similarities

Breakdown the problem into workable modules
  – Alert Visualization (AlertViz) provides global alert visualization
  – Exploration Visualization (ExViz) provides the same data with queried data for specific time frames
  – Connection Visualization (ConnViz) provides connection log visualization in a grid sorted by Source (Src) or Destination (Dst) Internet Protocol (IP) on one axis, time on a second axis, and quantity of connections in the third axis

Prioritize development focus based on requirements

Design to Concept - Provide a viable 3D-display prototype to meet network operational needs

Interactive development – Frequent updates – Quick turn around
Integration

IWViz
• 3D Visualization
• Situational Awareness

IWQuery
• Interface between system components
• Query capability

Sensors
• Intrusion Detection
• Generates alerts

Parts & People Working As A Whole

Director
• Stores alert information
• Provides detailed alert information
AlertViz

- Represent Alerts:
  - Cubes over designated sites
  - Information Window containing relevant alert data
  - Date and time of last alerts received and destination location indicator

- Usability:
  - Configurable files for tailoring
    - Filter designators and descriptors
    - Coordinates (e.g., site latitude/longitude)
    - Sensor collectors
    - Hot IP list with blinking option
  - User selectable color coding
  - Point and click/auto data fill
  - User defined profiles
  - Visual sizing

- Alerts filtered on:
  - String Match Events (e.g., BAD_PASSWORDS)
  - Events (e.g., Distributed Port Probe)
  - Protocols (e.g., Transmission Control Protocol [TCP])
  - Source or Destination IP
  - Area of Responsibility (AOR)
  - Sensor

General Information Window

Area of Responsibility Toolkit Page

Events Toolkit Page
ExViz

- Includes all functional capabilities included on the AlertViz module as well as:
  - Information Window containing bytes sent and received
  - Date and time of last alerts received and destination location indicator
- Query capability on:
  - Source IP/Destination IP
  - Date
  - Time range
  - Status
  - Bytes transferred
  - Destination Port #

- Alerts filtered on:
  - Capabilities included on the AlertViz module
  - Zero Bytes Filtering
## IWViz Functionality

- **Installation**
- **Configuration**
- **Starting Up**
- **Shutdown**
- **Modules**
- **Popup Menubar Operations**
- **File Options**
- **Profile Options**
- **Tools Options**
- **Display Options**
- **Filters Options**
- **Windows**
- **Navigation & User Interface**
- **Maintenance**

### Test Areas Covered

- **Module**
  - AlertViz (A)
  - ExViz (E)
  - ConnViz (C)

- **Unit**
  - Date
  - Pass / Fail
  - Tester

- **System**
  - Date
  - Pass / Fail
  - Tester

- **Government Acceptance**
  - Date
  - Yes / No
  - Approver

- **User Acceptance**
  - Date
  - Yes / No
  - Approver

### Test Results

<table>
<thead>
<tr>
<th>Module</th>
<th>AlertViz (A)</th>
<th>ExViz (E)</th>
<th>ConnViz (C)</th>
<th>Date</th>
<th>Pass / Fail</th>
<th>Tester</th>
<th>System</th>
<th>Government Acceptance</th>
<th>User Acceptance</th>
</tr>
</thead>
<tbody>
<tr>
<td>Test 1</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>01/01/2023</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Test 2</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>02/02/2023</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

© 2006 The MITRE Corporation. All rights reserved.
Fielding and Deployment Activities

- **Pre-Deployment Activities (Preparation)**
  - Coordination activities
  - Build contact list and locations
  - Interim Certificate to Operate (ICtO) approval
  - Prepare platform and support documents
  - Survey requesting configuration information
  - Baseline software
  - Coordinate travel with Points of Contact (POCs)
  - Accreditation

- **Deployment Activities (Fielding)**
  - General briefing
  - Check setup and configuration (e.g., Director connection)
  - Test run setup
  - Train target users
  - Review System Change Request (SCR) process
  - Question and Answer (Q&A)/collect initial comments
  - Out brief

- **Post-Deployment Activities (Sustainment)**
  - Update deployment process
  - Prepare after action report
  - Follow-up on submitted enhancements
  - Send out software and documentation updates to deployed locations
  - Review CND visualization needs and support options
  - Provide maintenance and help desk support
  - Finalize documentation – worked throughout process
Deployment Rationale

- IWViz offers capabilities not available in Commercial-Off-The-Shelf (COTS) software
- No licensing fees
- Satisfies Intrusion Detection System (IDS) related visualization requirements
- Conditions—Provides prototypes to users “as is” with ongoing support from government sponsor until successful sustainment transition occurs, currently:
  - Working assessment of network impact or interoperability—None expected or experienced in the laboratory operation
  - User’s manual provided—Includes setup directions
  - Training provided—Initially at deployment, On-The-Job, Call in technical support
  - Initial load and configuration—Users to support updates and new version installs
Technology Transfer

- IWViz moved from the prototype stage and was ready to migrate to an operational technology
  - MITRE not chartered or staffed to provide product sustainment
  - Necessary to implement an IWViz technology transfer plan

- Options
  - Commercial License – Nonexclusive: Can require them to give back copies
    - We transfer the software directly to selected companies
    - Sponsor transfers the software to contractors and/or companies
  - Open Source
    - Need Public Release
    - Open to all folks national and abroad
    - Hard to track who has it
  - Cooperative Research And Development Agreement (CRADA) – Joint government/industry R&D partnerships which share resources
  - Industry Standards – Influence
  - External Publications – Public domain

- Concerns
  - Intellectual Property
  - Conflict of Interest
  - Legal & Ethical (Contact)
  - Lose of Direction

- Select best way forward
  - Which is the easiest and least confining?
  - Which ones do we want to pursue, could be one or many?
Growing Interest in Technology Transfer

- Venture investors looking for solid technology underpinnings in investment opportunities—reaction to dot com era mistakes
- Research institutions increasingly willing to partner with venture community for additional revenue opportunities
- Homeland Security and other government initiatives driving interest in potential applications of advanced technologies being developed in research institutions
- Mid-Atlantic technology commercialization organizations ideally positioned at the crossroads of industry and government technology hubs
- Tech transfer still relatively new (Bayh-Dole Act passed in 1980)
Alert Visualization (AlertViz)

Real time situational awareness allowing for quicker response in decision making

Allows for initial situational assessment and predictive support
Primary Support Team

- Therese Metcalf—Technical Lead-MITRE
- Ken Beyer—Government Project Lead
- Dr. Mike Wingfield—Lead Developer-MITRE
- Tim Farias—Testing & Technical Support-MITRE
- Interface Developer—Varied Government Support
- Users—Government Personnel