The Future of Protocol and SMB2/3 Analysis

Paul Long
Dave MacDonald
Microsoft
The Protocol Engineering Framework

PEF enables teams to formally describe their protocol with “One Truth,” and to generate a consistent set of artifacts from that model with very little additional effort.
## The Protocol Engineering Framework

<table>
<thead>
<tr>
<th>Functions</th>
<th>Value Propositions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Visually explore and validate state machines</td>
<td>Improve protocol design efficiency</td>
</tr>
<tr>
<td>Generate documents, code contracts, and parsers</td>
<td>Improve efficiency of producing accurate, verifiable protocol documentation</td>
</tr>
<tr>
<td>Generate test suites that run against implementations</td>
<td>Improve conformance test efficiency and coverage</td>
</tr>
<tr>
<td>Integrate event and protocol message tracing</td>
<td>Improve diagnosis and debugging of platforms and services</td>
</tr>
<tr>
<td>Machine validation of protocol traces</td>
<td>Improve protocol interoperability</td>
</tr>
</tbody>
</table>
Microsoft Message Analyzer

A modern message analysis tool built on PEF with:

- Flexible, multi-layer and endpoint tracing
  - Packet inspection in Windows at NDIS, Firewall Stack, HTTP Proxy
  - Events and messages from any Event Tracing for Windows (ETW) provider
  - Support for “Trace Scenarios”: groups of providers with filters
- Analysis and validation of virtually any message type
  - Network packets – Protocol Data Units
  - ETW events – described by manifests imbedded in components
  - Text logs – described by text input adapter configuration files
  - Other sources – “input adapters” can be added for any other message
  - Support for validation of message structure, behavior, and architecture

All mingled together, and grouped/sorted however you want
Microsoft Message Analyzer

Powerful, extensible viewing and analysis

- **Browse, Select, View**
  - Browse for messages from various sources (live, or stored)
  - Select a set of messages from those sources by characteristic(s)
  - View messages in a provided viewer, configure or build your own

- **A new high-level grid view**
  - High level “Operations” view with automatic re-assembly
  - “Bubbling up” of errors in the stack to the top level
  - Ability to drill down the stack to underlying messages and/or packets
  - On the fly grouping, filtering, finding, or sorting by any message property
  - Payload rendering

- **Validation of message structures, behavior, and architecture**
  - Does the protocol comply with the specifications?
Demo – SMB2 analysis

- Start a Link Layer trace with SMB2 filter and analysis grid
- Demonstrate:
  - Trace Scenarios
  - Grouping
  - Manage Columns
  - Operations
  - Time Elapsed
  - Request/Response
  - Message Details
    - Stack View
    - Details View
    - Validation/Diagnosis Errors
Demo – Encrypted Traces

- Capture encrypted traffic with Firewall and SMB Provider trace scenarios
- Demonstrate:
  - Building a custom scenario
  - Capture with SMB Client Provider Trace with Firewall
  - Searching using **contains “SomeText”** (file name)
  - Capture State/Debugging Info
  - Grouping by SMB2.Header.SessionId
  - Filtering with **SMB2.smbfilename contains “MyFile”**
  - How traffic from two providers is related
Demo – Browse, Select, View

- Examine a Wireshark capture and SAMBA Log file together
- Demonstrates:
  - Browse, Select, View paradigm
  - Discuss Selection Timeline
  - Right Click SMB module add as filter
  - Right Click SambaSysLog add as filter
  - Details of SambaSysLog message
  - Adding a column for SMB Source_file
  - Loading a Saved layout
  - Sorting by Time
  - How messages are lined up next to each other
Demo – SMB Performance

- Using visualizers with Browse, Select View to understand SMB performance.

- Demonstrates:
  - Adding a selection filter for SMB2
  - Launch SMB summary view directly
  - How to analyze performance using a line graph visualizer
  - Demonstrate Time Slider to zoom in
  - Hover over points to display message data
  - Launching analysis grid based on visualizer element (double click line)
  - Tearing off of Tab to view side by side
Demo – Module View/General Usage

- Use Protocol Dashboard, Grouping, and Column Filtering

- Demonstrates:
  - Start a Firewall Trace
  - Protocol Dashboard
  - Multi-level grouping of Network/Transport layers
  - Quick column Filter Using Source Address “192.168.”
  - Quick column filter in summary
Demo – HTTP Proxy

- Showing HTTP text and image data in a rendered format
- Demonstrates:
  - Performance improvements when you capture HTTP
  - Handling of HTTPS encrypted data
  - Grouping by ContentType with right click
  - Using data rendering to view images
Next?

- Explore Message Analyzer (wrist band)
- Join our Connect Community
  - [https://connect.microsoft.com/site216/](https://connect.microsoft.com/site216/)
- File Bugs and Provide Feedback
Questions
Appendix – Visual Capability Reference

Following slides contain screen shots with descriptions of Message Analyzer Capabilities
<table>
<thead>
<tr>
<th>MessageNumber</th>
<th>Timestamp</th>
<th>Source</th>
<th>Destination</th>
<th>Module</th>
<th>Summary</th>
</tr>
</thead>
<tbody>
<tr>
<td>1607</td>
<td>08/27/2012 12:40:35.5780365</td>
<td>167.234.65.36</td>
<td><a href="http://www.bing.com">www.bing.com</a></td>
<td>HTTP</td>
<td>GET <a href="http://www.bing.com/fsi/11jE12204b701c344f43b86c88f02af4d4f8c2b5wV4&amp;event=CPT&amp;QAT">http://www.bing.com/fsi/11jE12204b701c344f43b86c88f02af4d4f8c2b5wV4&amp;event=CPT&amp;QAT</a></td>
</tr>
</tbody>
</table>
Diagnosis and Validation

"Bubbling Up" Errors

Grouping
Multi-level Grouping

Column Chooser with Search

Details and Data Views Collapsible

Column Chooser with Search

Details and Data Views Collapsible
Browse->Select->View

Traces and log files

Time Range Selector (Beta for text logs only)

Select messages by characteristics

Microsoft Message Analyzer
Session Explorer
Multiple Views

Bytes/Second for SMB Reads and Writes

Case-specific viewers

Bytes Sent for SMB Reads and Writes - Count, Average, Max

SMBFileName  Count  Average  Max
 davemacd\SMB2Test.cap  34  62362.3529411765  65536

Start: 05:11:04.670  End: 05:11:04.676
Start: 05:11:01.888  End: 05:11:04.676
Appendix – PEF Details
Open Protocol Notation (OPN)
- Formal human and machine readable protocol specification language
- Description of structures, behavior, data, and architecture
- Full-fidelity textual representation of an object model

Protocol Engineering Framework (PEF)
- A full tool chain based on OPN
- Artifacts
  - Technical Documents (TDs)
  - Visual protocol models and exploration
  - Test suite generation
  - Runtime monitoring capability
  - Validation of traces against specs
  - IDL
Migrating an existing set of protocols to OPN

Bootstrap from existing code, and use the authoring environment for any subsequent update
Producing and Maintaining Documentation

- Specifications are generated from OPN
- Writers add “prose” which is stored separately
- Generated and written content are merged
Generating protocol test suites

- Select paths through the model
  - Assisted parameter generation, path coverage
  - Push-button test sequence generation