Microsoft

Advances in Network Capture of SMB2/3

SambaXP

May 2013

Neil Martin, Test Manager
Interoperability and Tools
Windows Server & System Center

Introduction

- Interoperability & Tools Group
- Existing Network Packet Capture Tools
- Challenges for existing tools
- Microsoft Message Analyzer

Interop and Tools

- What we do
  - Part of Windows Server Org
  - Develop Linux Kernel drivers for Hyper-V
    - (Known as **Linux Integration Services)**
  - Develop *NIX agents for System Center for management of non windows O/S
  - Develop and maintain CoApp – Open Source package management for Windows
    - http://CoApp.org
  - Develop and maintain Microsoft contribution to OpenStack
  - Manage and coordinate publication of Microsoft protocol documentation
  - Develop protocol test suits for key protocols
  - Developed Microsoft Network Monitor (sniffer)
    - http://www.microsoft.com/en-us/download/details.aspx?id=4865
  - Developing Microsoft Message Analyzer (more on this)
  - Manage plug-fest and interop events for Microsoft

Windows Protocols

- Over 450 published specifications for Windows Protocols
  - (as of Windows 8)
  - (http://msdn.microsoft.com/en-us/library/gg685446.aspx)
  - Available online and as PDF
  - Continue to publish new documents with each release of Windows
  - Publish Overview Documents for protocol collections
- Continue to develop tools and technology to aid with the development of protocol documents, parsers and test technology to aid interoperability

Practical Interoperability

- Microsoft hosts numerous events
  - Most popular are:
    - File and Print Protocols
    - Identity
    - Remote Desktop
- Attend industry events
  - SNIA/SDC Santa Clara is a popular file sharing protocol event
- Network sniffing/capture and analysis tools are important tools for interoperability

Existing Network Packet Capture Tools

- Often called network sniffers or packet analyzers, some examples are:
  - Microsoft Network Monitor
  - WireShark (previously known as Ethereal)
  - Tpcdump
  - Pcap/winpcap
  - Many others ….
- The tools typically capture network packets at the NDIS layer
  - (NDIS - Network Driver Interface Specification)
  - Can be thought of as an API for a Network Interface Card (NIC)
- These tools have parsers that allow for identification and dissection of network protocols

Challenges faced by Existing Tools

- Increasing Network Speed and Data Size
  - SMB Direct, RDMA, Infiniband, etc..
    - 10 gig/sec and then some ……..
- Alternative Data Sources
  - RDMA, USB, Phone, Blue Tooth, Logs, etc.
- Increased complexity
  - Data Centers, Clustering`
- Security and privacy concerns
  - Network captures left on support engineers machines
  - User data sent to services

Microsoft Message Analyzer

- Next Generation NetMon
- File compatible with WireShark and Netmon, pcap and NM cap files
- Addressing many of the technical challenges of modern networks
  - Pattern matching
  - Protocol Validation
  - Multiple Viewers
  - Data capture from multiple sources
  - Header only network capture
  - Correlation of data across multiple data sources and logs
  - Database storage for network and other trace sources
  - OPN Parser language

Microsoft Message Analyzer

- 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

Data Capture from Multiple Sources

- Message Analyzer captures ETW
  - ETW - Event Trace for Windows

- Message Capture from:
  - Traditional NDIS traffic from the Network Adapter
  - Windows Filtering Platform
  - Web proxy
  - USB ports
  - Bluetooth
  - Windows SMB Client
  - Windows SMB Server ……

Microsoft Message Analyzer

- 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?

Event Tracing for Windows

- ETW allows capture from ETW providers
  - May be traditional NDIS
  - Firewall
  - HTTP proxy
  - Other ETW providers
  - Enables capture of encrypted traffic within SMB2 server

Traditional NDIS Capture and more

- Message Analyzer can capture at the NDIS layer and
  - Has a web proxy for HTTP work
  - Has a Windows Firewall Layer for additional functionality
    - Loop back adapter
    - Deals with some encryption

Header only Network Capture

- Capture protocol header
- Discard payload
- Obtains substantial savings in capture sizes
- Currently limited set of protocols
  - TCP, Ethernet, HTTP, SMB2, etc..

Download and Join our Community

- Invite you to Explore Message Analyzer
- Connect Community
  - https://connect.microsoft.com/site216/
- Download on downloads link (for free)
- Do need a Microsoft liveid for login
  - RTM version will be on download center

Questions and Answers

Demo – SMB2/3 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

Demo – Browse, Select, View

- Demonstrates:
  - Browse, Select, View paradigm
  - Discuss Selection Timeline
  - Right Click SMB module add as filter
  - 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