Prerequisites

Interest in software diagnostics and in general systems theory
Software Diagnostics

Problem

Software Diagnostics

Problem$_1$

Problem$_2$

Problem$_3$

Software Problem Solving
Why?

- Organized Complexity of Software
- Software as Human Artifact
- Problem Solving
Goals

- Ideas from General Systems-Theory
- Applications to Software Diagnostics
Software Diagnostics

- Pattern-driven
- Systems approach
System and Environment

- Not My Version
- Changed Environment
- Hooksware
Using Humanities (Past)
Using Humanities (Now)

Software System ↔ Modeling ↔ Humans
Using Humanities (Example)
Isomorphic Systems
Isomorphic Patterns

- Software Traces
- Windows Patterns
- Narrative Story
- Mac OS X Patterns

\[ f \quad f^{-1} \quad g \quad g^{-1} \]
Isomorphic Diagnostics

Software Traces \( \iff \) Memory Dumps

\( f \) \( f^{-1} \)
Isomorphic Diagnostics 2

Software Traces \( \xrightarrow{f} \) Network Traces
\( \xleftarrow{f^{-1}} \)

Network Trace Analysis Patterns
Isomorphic Disciplines

Metaphorical Bijection
Metaphorical Bijection

Software Narratology \[ f \] Narratology

Software Narratology
Complementarity (Artifacts)

Quantum Mechanics and observables: $x / p_x$

- Memory Dump
- Software Trace
Complementarity (Reports)

Solution: Pattern Checklists
Complementarity (Analysis)

Malware

Victimware
Decomposition of Behavior

- GUI state changes
- GUI messages
- Product specific messages
- System messages
- Memory dumps
- Network traces
- Screenshots
Holistic Approach

- Complete (or fiber bundled) dump
  - All processes and threads

- Full trace
  - All modules
Diagnostics Complexity

Memory Dump Analysis

\[ C \sim F \left( C_{\text{Mem}}, C^{-1}_{\text{Tool}}, C^{-1}_{\text{Pat}} \right) \]

- \( C_{\text{Mem}} \): structural complexity
- \( C_{\text{Tool}} \): the number of commands
- \( C_{\text{Pat}} \): the number of patterns in a catalog
First Fault Diagnosis

- Most diagnostic patterns are first fault
- First fault vs. second fault tools
Software Diagnostics Tools

Software Diagnostics Workbench
Diagnostics by Mhole 😊

HUMINT and SIGINT approach to software diagnostics
(moles or memory holes)

Mhole In a Whole
Further Reading

Systems Thinking and Science

- An Introduction to General Systems Thinking (by Weinberg)
- Facets of Systems Science (by Klr)

Software Diagnostics

- Software Diagnostics Institute
- Memory Dump Analysis Anthology: Volumes 1, 2, 3, 4, 5, 6, 7, …
  Volume 6 is in preparation (September, 2012)
  Volume 7 is planned for the end of 2012
- Software Trace and Memory Dump Analysis: Patterns, Tools, Processes and Best Practices
- Introduction to Pattern-Driven Software Problem Solving
- Introduction to Software Narratology
- Introduction to Pattern-Driven Software Diagnostics
- Victimware
Next Webinar

Abductive Reasoning in Software Diagnostics

December, 2012
Q&A

Please send your feedback using the contact form on DumpAnalysis.com
Thank you for attendance!