Real Insight from Code to Silicon

SourcePoint™  ScanWorks®

JTAG Debug of Windows Hyper-V / Secure Kernel with WinDbg and EXDI

REcon 2024

Alan Sguigna, Ivan Rouzanov

June 29, 2024

Workshop Announcement – Soprano A

- SourcePoint debuggers connected to live Intel targets!
- First come, first served
- 3:30pm – 4:30pm: 10 seats
- 4:30pm – 5:30pm: 10 seats
- Basic knowledge of WinDbg/Hyper-V recommended
- Sign-in sheet available after this session
- ***Complete systems available to take home***

Agenda

- SourcePoint JTAG-based debugger
  - From UEFI to Windows
- Combining WinDbg + SourcePoint
  - OS-aware + JTAG/ Hardware Tracing
- Demo configuration
  - What you'll see in the demo
- Demo
- Wrap-Up

SourcePoint: x86 JTAG-based debugger

- Collaboration with Intel for 20 years
- Merger with Arium in 2013
- Best-in-class UEFI debugger
- Support for x86: Intel (all CPUs) and AMD (EPYC)
- Source-level symbolic debugger, full run-control (stop, go, single-step, breakpoints, etc.)
- Supports innovative Trace features on Intel

SourcePoint JTAG-based debugger: a little history

UEFI – circa 2008

Run-control

Intel Trace Hub

Intel Processor Trace

Architectural Event Trace (AET)

SMM breakpoints (Entry, Exit, Data, I/O)

Reset/Init/Power Cycle breakpoints

Macro Language

XDP and DCI access

Windows (et al) – circa 2023

EXDI integration with WinDbg

Hypervisor BP (VM Launch, Resume, Exit)

VMCS Viewer/ Editor

JTAG

“Ring -∞”

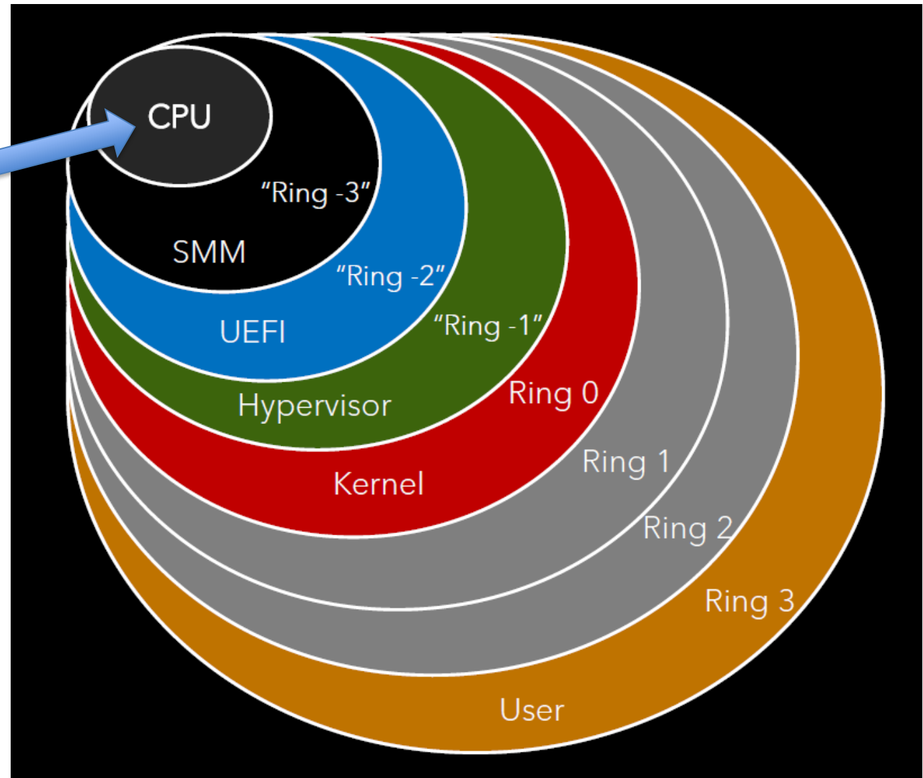
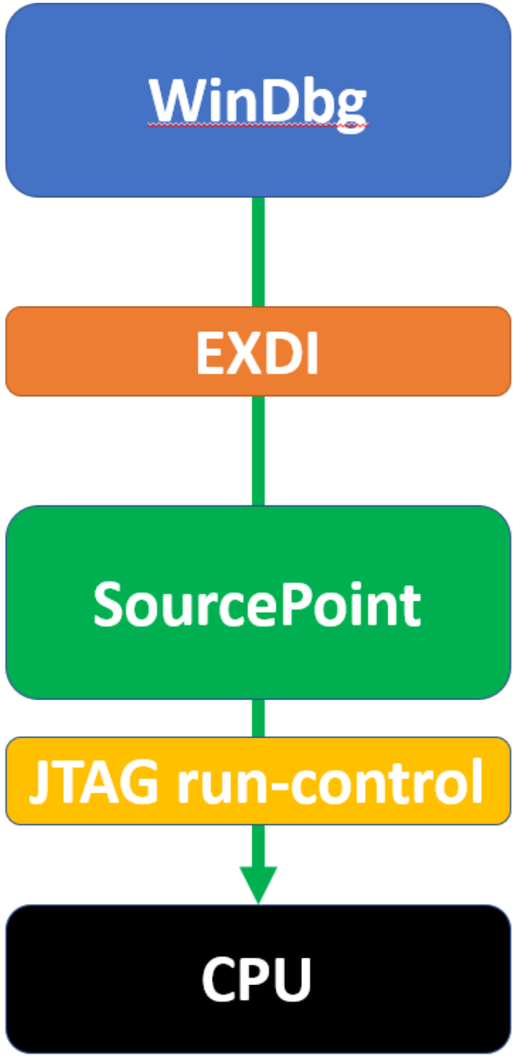


Image courtesy of Pavel Yosifovich, Windows Internals course

SourcePoint™
Platform for Software Debug and Trace

Why combine WinDbg and SourcePoint?

- Recent update to EXDI (Extended Debug Interface)
- EXDI is an adaptation layer between a software debugger and a debugging target.
- Extends WinDbg by adding support for hardware-based debuggers (i.e. JTAG-based)
- WinDbg is the controller; SourcePoint is the worker
- “Debugging the Undebuggable” https://www.andrea-allievi.com/blog/debugging-the-undebuggable-part-1/
  But on steroids!



Why is this cool? New Capabilities

- No agent on the target!
- Target runs at native speed
- Debugging from reset vector to Windows: UEFI + Windows
- VM Launch/ Resume/ Exit breakpoints: hvix64 -> hvloader -> securekernel and beyond
- Static and dynamic analysis of the Secure Kernel with symbols
- VMCS Viewer/Editor
- Intel Processor Trace (Intel PT)
  - Disabling Windows mitigations; i.e. Intel PT “conceal bits”
- Architectural Event Trace (AET)
- Debugging VBS-enabled enclave code
- No NDA

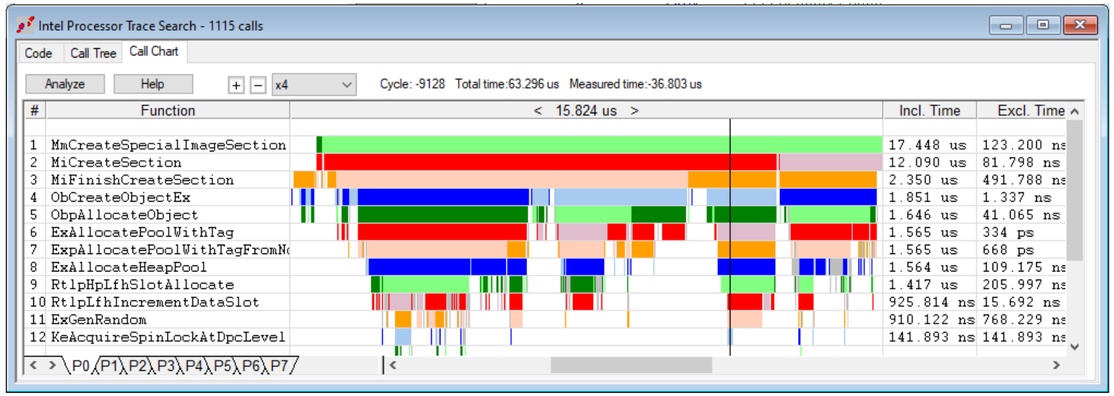
Hardware Tracing Secret Weapons: Intel PT and AET

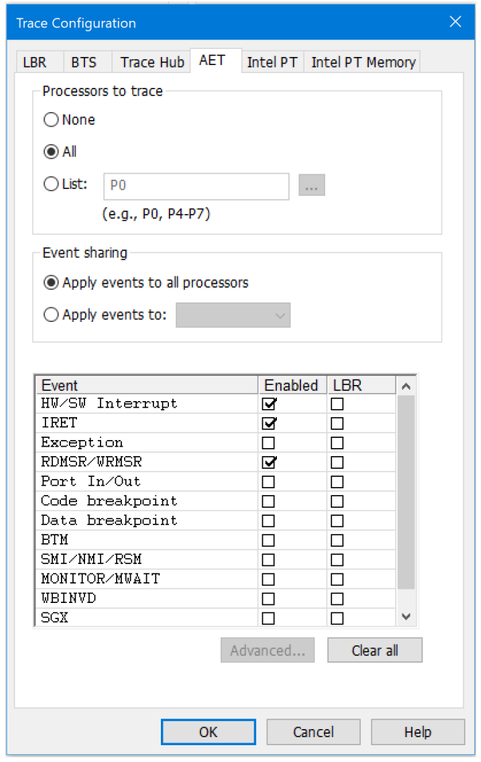
Intel PT

- Instruction trace, captured to target system memory
- Nominal overhead (1% - 3%)
- Can filter by CR3, CPL, address

AET

- Event trace; supports probe mode (JTAG) only
- Captured to DCI, MTB, or System Memory
- Not CR3-aware





AAEON UP Xtreme i11 (Tiger Lake)

- Debugging on a physical target
- Supports Intel DCI (no HW probe required) out of the box
- All Intel run-control and trace features supported

Microsoft Azure Certified

UP Xtreme i11 - 0000 Version Board Series

As low as **$299.00** (Excl. Tax) SKU#: UPX-TGL-0000

Processor

Intel® Celeron 6305E | Intel® Core™ i3-1115GRE | Intel® Core™ i5-1145GRE | Intel® Core™ i7-1185GRE

Memory

via 2x SO-DIMM DDR4*

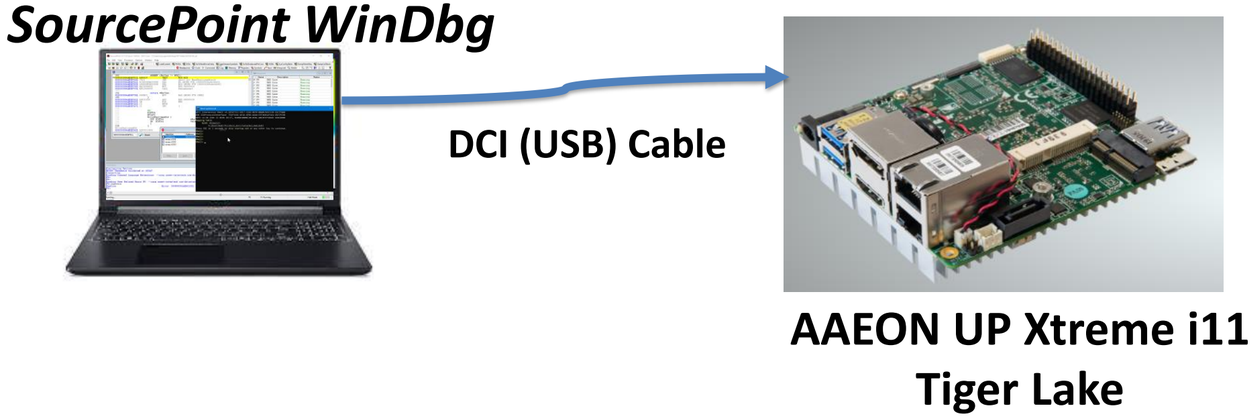
eMMC / Storage

via SATA or M.2 2280 NVMe*

Software Preinstallation Service

The Demos – what you'll see

1. Alan: Secure Kernel debug, VBS-enabled enclaves, Intel PT, AET, NTOS <-> SK "dance", etc.
2. Ivan: practical use of Intel PT + AET



Demo

Resources

- SourcePoint Academy: https://www.asset-intertech.com/resources/academy/sourcepoint-academy/
  - *SourcePoint WinDbg Getting Started Guide*
  - *Getting Started Guide for the AAEON UP Xtreme i11*
  - *Videos, Online Help, Release Notes, etc.*
- Getting a copy: https://www.asset-intertech.com/products/sourcepoint/sourcepoint-windbg/

Wrap-Up and Contact Information

Available Now

SourcePoint Home: emailto:ai-info@asset-intertech.com

SourcePoint Enterprise: www.asset-intertech.com/contact-us/

'X' DM @AlanSguigna

or LinkedIn InMail

Real Insight from Code to Silicon

SourcePoint™
Platform for Software Debug and Trace

ScanWorks®
Platform for Embedded Instruments