15-612 Operating System Practicum

KDD (Windows Debugger Stub) enhancements

Julian Tuminaro (jtuminar)
Jenish Rakholiya (jrakholi)

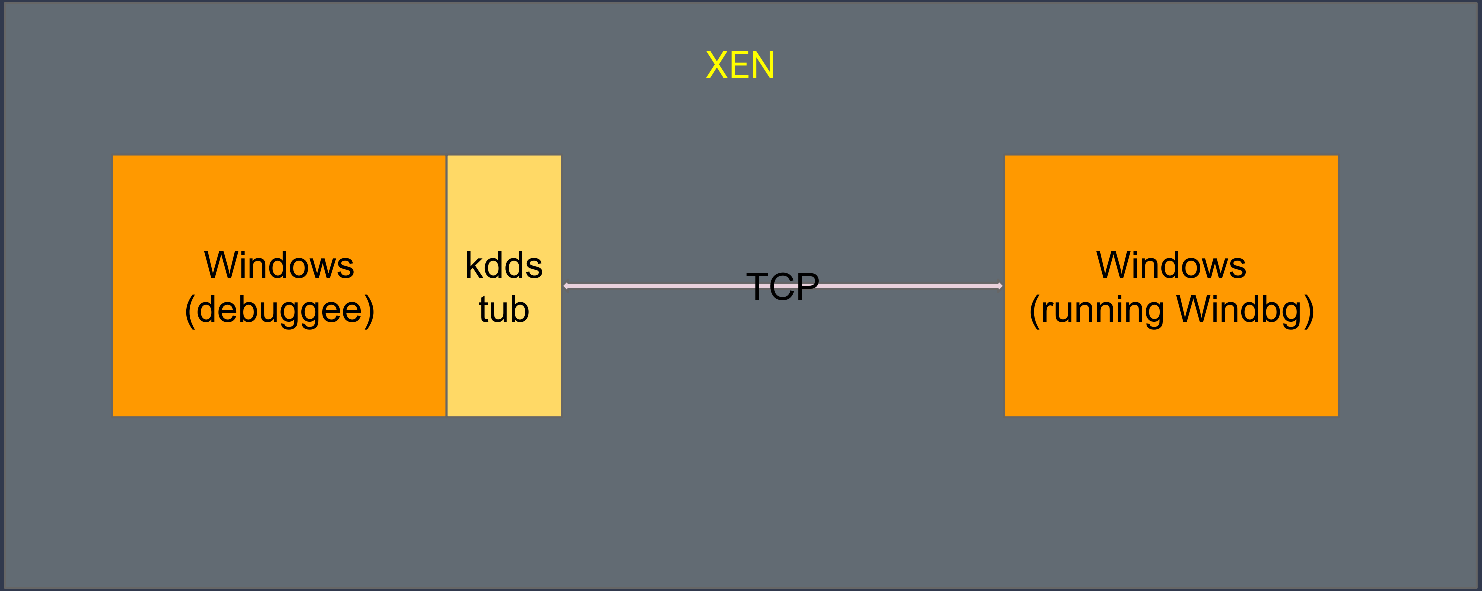
Xen

- Type-1 hypervisor
- Supports paravirtualization and hardware-assisted virtualization on x86 mainly

Project Idea

- Want to debug Windows Kernel using WinDbg without enabling debugger enabled mode (without letting kernel know it is being debugged) in Windows kernel while booting

- Add support for Windows 8.1 and later



XEN

Windows
(debuggee)

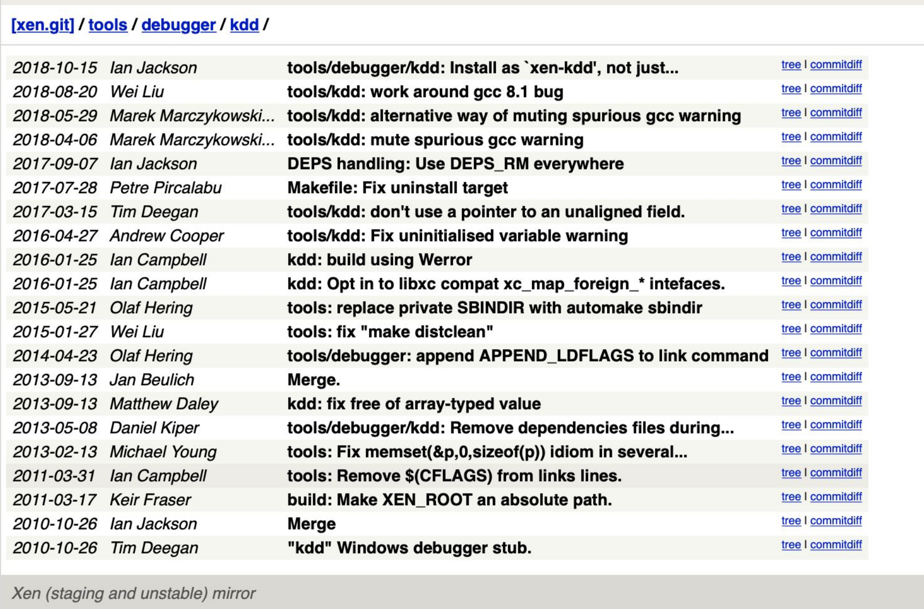
kdds
tub

TCP

Windows
(running Windbg)

Current Status

- Supposedly works up to Windows 7 SP 1
- 1,700 lines of kdd stub code which hasn’t been touched in a long time (like 9 years)



[xen.git] / tools / debugger / kdd /

2018-10-15	Ian Jackson	tools/debugger/kdd: Install as `xen-kdd', not just...	tree | commitdiff
2018-08-20	Wei Liu	tools/kdd: work around gcc 8.1 bug	tree | commitdiff
2018-05-29	Marek Marczykowski...	tools/kdd: alternative way of muting spurious gcc warning	tree | commitdiff
2018-04-06	Marek Marczykowski...	tools/kdd: mute spurious gcc warning	tree | commitdiff
2017-09-07	Ian Jackson	DEPS handling: Use DEPS_RM everywhere	tree | commitdiff
2017-07-28	Petre Pircalabu	Makefile: Fix uninstall target	tree | commitdiff
2017-03-15	Tim Deegan	tools/kdd: don't use a pointer to an unaligned field.	tree | commitdiff
2016-04-27	Andrew Cooper	tools/kdd: Fix uninitialised variable warning	tree | commitdiff
2016-01-25	Ian Campbell	kdd: build using Werror	tree | commitdiff
2016-01-25	Ian Campbell	kdd: Opt in to libxc compat xc_map_foreign_* intefaces.	tree | commitdiff
2015-05-21	Olaf Hering	tools: replace private SBINDIR with automake sbindir	tree | commitdiff
2015-01-27	Wei Liu	tools: fix "make distclean"	tree | commitdiff
2014-04-23	Olaf Hering	tools/debugger: append APPEND_LDFLAGS to link command	tree | commitdiff
2013-09-13	Jan Beulich	Merge.	tree | commitdiff
2013-09-13	Matthew Daley	kdd: fix free of array-typed value	tree | commitdiff
2013-05-08	Daniel Kiper	tools/debugger/kdd: Remove dependencies files during...	tree | commitdiff
2013-02-13	Michael Young	tools: Fix memset(&p,0,sizeof(p)) idiom in several...	tree | commitdiff
2011-03-31	Ian Campbell	tools: Remove $(CFLAGS) from links lines.	tree | commitdiff
2011-03-17	Keir Fraser	build: Make XEN_ROOT an absolute path.	tree | commitdiff
2010-10-26	Ian Jackson	Merge	tree | commitdiff
2010-10-26	Tim Deegan	"kdd" Windows debugger stub.	tree | commitdiff

Xen (staging and unstable) mirror

What we want future to look like?

- Support for Windows 8.1 and 10 (x86 and x86_64) to kdd

- Support for Windows Server 2012 to kdd

- kdd allows WinDbg to write out usable Windows memory dumps for all supported versions

- Provide user guide for kdd on Xen wiki

- Other surprises

Who is working on having similar future?

- qemu (at least one guy is)
- Wireshark Dissector of KD Protocol
- Radare2 debugger
- Vmware

Lines of Code

Currently:

/xen/tools/debugger/kdd.c: ~ 1, 100 lines

/xen/tools/debugger/xen-kdd.c: ~650 lines

- Most will still be useful, ~1,500 lines

Expecting to add:

/xen/tools/debugger/kdd.c: ~ 1,000 lines

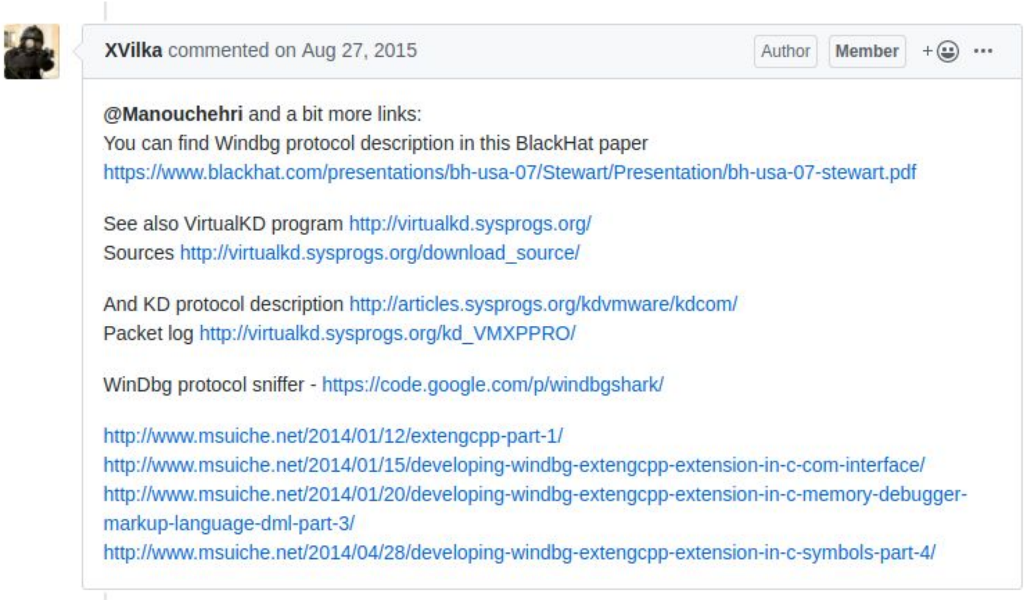
/xen/tools/debugger/xen-kdd.c: ~ 700 lines

Qemu WIP:

3,600 lines of code (including headers and Makefile)

Resources

- QEMU WIP for Windbg
  - https://github.com/patchew-project/qem
    u/compare/80422b0...fe77421
- Radare2 WIP for Windbg
  - https://github.com/radareorg/radare2/is
    sues/1246?fbclid=IwAR3TaRogVIZKVcU
    jtfk-MXtUGyAxCZ1hZ_Pj_MDg03UGDTni
    TLBQ52Cm0
- Wireshark dissector for KD Protocol
  - https://github.com/Lekensteyn/kdnet



XVilka commented on Aug 27, 2015

@Manouchehri and a bit more links:
You can find Windbg protocol description in this BlackHat paper
https://www.blackhat.com/presentations/bh-usa-07/Stewart/Presentation/bh-usa-07-stewart.pdf

See also VirtualKD program http://virtualkd.sysprogs.org/
Sources http://virtualkd.sysprogs.org/download_source/

And KD protocol description http://articles.sysprogs.org/kdvmware/kdcom/
Packet log http://virtualkd.sysprogs.org/kd_VMXPPRO/

WinDbg protocol sniffer - https://code.google.com/p/windbgshark/

http://www.msuiche.net/2014/01/12/extengcpp-part-1/
http://www.msuiche.net/2014/01/15/developing-windbg-extengcpp-extension-in-c-com-interface/
http://www.msuiche.net/2014/01/20/developing-windbg-extengcpp-extension-in-c-memory-debugger-markup-language-dml-part-3/
http://www.msuiche.net/2014/04/28/developing-windbg-extengcpp-extension-in-c-symbols-part-4/

Point of Contacts

- Paul Durrant - Coordinator for this GSoC project
    - Our main contact currently

- Tim Deegan - Wrote Original KDD implementation

- XVilka - Worked on supporting KD protocol in Radare

xvilka is a nice guy

Licenses

- Xen: GPLv2
- Qemu: GPLv2
- Radare2: GPLv3
- Windbg: Just don’t reverse it or distribute it
- kd dll/kd Protocol: Not quite sure, but there is a lot of research that has examined it

Standard Acceptance Process

1. Submit a patch. Follow these instructions: https://wiki.xenproject.org/wiki/Submitting_Xen_Project_Patches

2. Make sure to CC the maintainer, in our case it is: Tim Deegan

3. Assuming working code, maintainer will request some small fixes such as variable names, and formatting.

4. Get accepted.