Agenda and Minutes: x86 Community Call September 2018

No new items were added to the agenda. Minutes are added in blue. Closed ACTIONS in green.

August minutes were at
https://lists.xenproject.org/archives/html/xen-devel/2018-08/threads.html#01259

Attendees

Lars Kurth
Wei Liu, George Dunlap, Paul Durrant, Sergey Dyasli, Andy Cooper, Ian Jackson (Citrix)
Christopher Clark (OpenXT Project)
Doug Goldstein (Rackspace)
Brian Woods (AMD) - there was a Janek from AMD as well, but we didn't quite understand the name due to the line @Brian, please correct
Daniel Kiper (Oracle)
Tamas K Lengyel (AIS)
Daniel Smith (Apertus)
Jan Beulich, Juergen Gross, Dario Faggioli (Suse)
Please add your name to this list, if you were present at the call and are not on the list

Open / Closed Actions from Previous calls

- [Open] Lars to bring up x86 bottleneck at next AB call – due to the Aug holidays we didn't have any of the relevant vendors on the call
- [Open] Christopher will follow up on IRC/xen-devel@ re memory scrubbing
- [Closed] Andrew was going to look at L1TF related issues and add this to Jira (unless I misunderstood) See https://lists.xenproject.org/archives/html/xen-devel/2018-08/msg01160.html
- [Closed] Juergen to send a mail related to 32PV support to xen-devel See https://lists.xenproject.org/archives/html/xen-devel/2018-08/msg01230.html

Argo: Christopher Clark

"Argo" (formerly v4v) inter-VM communication mechanism for Xen 4.12, discussed at Xen Summit 2018 design session and PSEC 2018, design doc forthcoming. Varants of this technology have been used in OpenXT and uXen/Bromium for several years.
Video: https://www.platformsecuritysummit.com/2018/speaker/clark/
Wiki: https://wiki.xen.org/wiki/Argo:_Hypervisor-Mediated_Exchange_(HMX)_for_Xen

There was a brief discussion on time-line: Christopher is targeting 4.12. (R

ich Persaud has already replied on the mailing list to Juergen's last "Xen 4.12 Development Update" mail indicating this.) There was a brief discussion about the process and JIRA tickets.

Andy: mentioned that we should weed out some of the many old Xen JIRA tickets or come up with some classification. Right now, it is not clear as to what is relevant (aka what is a long term wishlist and what is more short-term)
ACTION: Lars would be happy to start a discussion on IRC, then xen-devel and start tidying the JIRA instance up

ACTION: Juergen agreed to add Argo to the work tracking list for the 4.12 release, communicated in the "Xen 4.12 Development Update" mail series.
ACTION: Lars to give Christopher write access to JIRA (done)
ACTION: Christopher to create a JIRA ticket for the Argo work.

Trenchboot: Daniel Smith

The presentation will provide a quick review of the concepts underlying integrity (trust) in the boot process used by SecureBoot and Measured Boot. From there, our focus will be on explaining the types of measured boot. Then we will touch on how TrenchBoot is working to make measured boot more accessible while still providing rich capabilities. Wrapping up we will discuss collaboration being sought with the Xen Project.

Daniel presented:
https://lists.xenproject.org/archives/html/xen-devel/2018-09/pdfJzocNrrrcQ.pdf

Other relevant slides:
https://lists.xenproject.org/archives/html/xen-devel/2018-09/pdfQfm7BUrRMb.pdf and related talks on Xen and/or UEFI, from AIS, Dell, Intel, Oracle:
https://www.platformsecuritysummit.com/2018/topic/boot/

There was some discussion around who is doing what: I did not manage to capture this, but:

- Andy mentioned some of the secureboot related stuff he and others at Citrix are working on (but these have not yet been posted)
- There was some discussion about issues with nested virt
- There was some technical discussion, which I did not fully capture. In particular the Xen kexec entry, memory reservation and a new hypercall. I got the sense that there are no in-principle obstacles to implement any of these
- The proposed timeline is Xen 4.13, but so far the Xen related bits are not resourced

Code: see https://github.com/TrenchBoot/trenchboot

People in the Xen community interested in trench boot (and present on the call): Andrew Cooper, Doug Goldstein

AOB

None