Upgrading SONiC kernel to 3.16.0-5 or later versions

Motivation

Recent vulnerabilities in Linux kernel including Meltdown and Spectre will probably leak passwords and sensitive data.

1. Meltdown is a hardware vulnerability affecting Intel x86 microprocessors and some ARM-based microprocessors. It allows a rogue process to read any kernel memory, even when it is not authorized to do so. Debian has addressed the known Meltdown attack vectors, CVE-2017-5754 in Linux kernel 3.16.0-5.
2. Spectre breaks the isolation between different applications. CVE-2017-5715 and CVE-2017-5753 are the official references to Spectre. Debian is still open for this attack. Check the latest status.

SONiC is currently based on Debian Linux kernel 3.16.0-4 and has these vulnerabilities. To make SONiC switches secure in large scale cloud environment, we should take prompt actions to upgrade its kernel to latest kernel version and keep following up with future versions for security kernel patches.

Approach

SONiC uses Debian Linux kernel 3.16.0-4 for both base image and containers. There are several steps to upgrade SONiC to Linux kernel 3.16.0-5.

1. Upgrade base image to Linux kernel 3.16.0-5
2. Upgrade ASIC drivers to Linux kernel 3.16.0-5, since kernel ABI bump means that all the modules need to be rebuilt against the updated kernel (link)
3. Upgrade platform drivers (sensors/led/fan/...) to Linux kernel 3.16.0-5

Progress

What has been done so far

1. Built Debian Linux kernel 3.16.0-5.
    a. Code
    b. Build log
    c. Binary
2. Built a base image with Linux kernel 3.16.0-5
    a. Pull Request
    b. Binary

    c. Tested the basic Linux operations on one Mellanox platform, no SONiC operations tested

3. Recompiled Opennsl
    a. Binary
    b. Tested the SONiC operations and on one Broadcom platform
4. Built several open source kernel modules (igb/ixgb) with Linux kernel 3.16.0-5
    a. Pull Request

Ongoing source code and images

- Target SONiC branch is an personal branch.
- Testing SONiC images are built in the [pull request](https://github.com/Azure/sonic-buildimage/pull/1294) webpage. You may find it at the 'Details' links, or in the popup menu when you click the ✓ or ✗ symbol after the last commit

Development model

1. New contributions should be submitted against above personal branch, so merged contributions will appear in above pull request and trigger pull request build automatically. You can think this as pull request to pull request.
2. Reviewing and merging will happens on the personal repo
3. The branch will be periodically (1~2 weeks) or on-demand rebased to Azure:master to sync with latest development
4. The branch will be merged to Azure:master after the majority of vendors verify their contributions working

Timeline

- Target finish within one month after Debian releases security patch, if the patch results in kernel version bump
    - CVE-2017-5754 releases on Jan 8, 2018
    - To be updated for future fixes

Call for Action

- Porting ASIC drivers to Linux kernel 3.16.0-5
    - ASIC vendors please submit PR against the personal branch
    - Microsoft will review and merge PR to the personal branch in personal repo
    - ASIC vendors please wait the original pull request build ready

    - ASIC vendors please fetch the newly built image in orignal pull request page.
    - ASIC vendors please validate the new image
- Porting other platform drivers to Linux kernel 3.16.0-5
    - Platform vendors please submit PR against the personal branch
    - Microsoft will review and merge PR to the personal branch in personal repo
    - Platform vendors please wait the original pull request build ready
    - Platform vendors please fetch the newly built image in orignal pull request page.
    - Platform vendors please validate the new image