Spectre and Meltdown Vulnerabilities, January 2018

Summary of Exploits
Computer security experts have discovered two major security flaws in the microprocessors inside nearly all of the world’s mobile devices, personal computers and servers running in cloud networks.

Back in June 2017, a security researcher named Jann Horn, working for Google’s Project Zero team, discovered a way for a sneaky program to steal information from parts of a computer that are supposed to be off limits. Horn and Project Zero notified the major vendors — Google, of course, as well as Intel, Microsoft, Apple, AMD, Mozilla, the Linux folks, Amazon and many more — and a quiet effort began to plug the security holes without alerting “the bad guys.”

Unfortunately, the issues were leaked a week early and computer vendors and operating system programmers are hurrying to catch up while the news tells everyone that the world is ending. For this reason, there’s a lot of information floating around, so hopefully the rest of this (rather lengthy) email will provide some answers.

As always, make sure your computers are fully patched. But this time, there’s a bit more involved...

Details
The Meltdown and Spectre issues take advantage of a modern CPU performance feature called speculative execution. Speculative execution improves speed by operating on multiple instructions at once—possibly in a different order than when they entered the CPU. To increase performance, the CPU predicts which path of a branch is most likely to be taken, and will speculatively continue execution down that path even before the branch is completed. If the prediction was wrong, this speculative execution is rolled back in a way that is intended to be invisible to software.

The Meltdown and Spectre exploitation techniques abuse speculative execution to access privileged memory—including that of the kernel—from a less-privileged user process such as a malicious app running on a device.

Translation, if bad code gets onto your computer, it can use these holes to make itself administrator and read data you’d rather it didn’t, like your passwords.

What systems are vulnerable?
The Meltdown flaw is specific to Intel (and some ARM chips we’ve now learned), but Spectre is a flaw in design that has been used by many processor manufacturers for decades. It affects virtually all microprocessors on the market, including chips made by AMD that share Intel’s design. Chips going back as far as 10 years might all be affected.
Because the issue is in the HARDWARE of the computer chips, rather than a bug in the operating system like most security that hits the news, there’s no simple fix, but everyone is working on ways to mitigate the issue.

Steps to Mitigation
In order to mitigate these issues, there are 3 types of upgrades that we’ll need (in order of priority) –
1. Updated browsers (critical)
2. Operating System patches
3. BIOS updates.

There is some talk in the news that some of these patches will result in your computer slowing down -- the entire purpose of “speculative execution” is to speed up your computer’s processing -- from 5% up to 30%, but ever since that announcement, we’ve been hearing that the reality, on desktop systems, is not quite that bad. A number of sources are saying that your average computer user won’t notice anything (so don’t worry about that at this point).

Browser updates are the most critical element as the easiest way to be impacted is through malicious Javascript on a website you go to...

- Google Chrome -- Chrome 64, due to be released on January 23, will contain mitigations to protect against exploitation. In the meantime, their recommendation is to upgrade to version 63.0.3239.132 (we’re pushing this now to all managed Windows and Macintosh computers) and enable their “site isolation” feature: “the Site Isolation protection loads each individual remote website in a separate process,” continued the <Google> spokesperson. “By doing so, if a user runs into an attack from a bad site, the process memory for the site the user is trying to reach is unavailable to be attacked. That way, your login secrets for one site cannot be stolen by another.” See https://support.google.com/chrome/a/answer/7581529 for details.

As this will cause a 10%-20% increase on memory usage for all computers using Chrome, and will cause some printing issues, campus is still discussing how to proceed. In the meantime, you can enable it yourself by upgrading to version 63.0.3239.132 and then in Chrome, go to the address chrome://flags/#enable-site-per-process and click “enable” on “Strict site isolation.” You’ll need to restart your browser, but otherwise that’s it.

- Mozilla Firefox -- with version 57.0.4, Mozilla Firefox has been updated to mitigate the impact of Spectre. We are pushing out this new version to our Windows and Macintosh computers. We recommend that you immediately update on personal computers.

- Internet Explorer / Edge -- Microsoft has released patches for Windows 10, Windows 8.1, and Windows 7 which are available now (if your campus machine is telling you it needs to reboot for patches, please do it soon).

- Safari -- If you’re still somehow running Safari on a non-Macintosh computer, remove it now. Apple stopped supporting Safari for Windows a long while back. Patches for Safari to fight Spectre have already been released for macOS 10.13, 10.12, and 10.11. Install them.

Operating Systems will also need to be patched to deal with these issues...
• macOS/iOS -- Please note that all MacOS systems and iOS devices are affected. Apple has already released mitigations in iOS 11.2, macOS 10.13.2, and tvOS 11.2 to help defend against Meltdown. Apple Watch is not affected by Meltdown.
  o Takeaway: Go update your Macintosh computers (personal and NCSU) by going to the App Store and downloading any patches you see there. Do that now. Install any patches you need on your iPads as well.
  o Caveat: Apple has updated High Sierra (10.13) to defend against Meltdown, but not Sierra (10.12). If you’ve not yet upgraded your personal machines to High Sierra, good time to do so. **We cannot upgrade our NCSU** computers due to an Antivirus issue -- we’re still waiting on Microsoft to release a new High Sierra version of our AV for Mac. But we’re also hearing that Apple will release Meltdown patches for Sierra in the coming week or two; Details:

• Windows -- Microsoft has already released patches for its Windows 10, Windows 8.1, and Windows 7 operating systems which we’ve pushed to campus machines. If your computer tells you that it needs to reboot for patches, please do it.
  o However, Microsoft halts AMD Meltdown and Spectre patches after reports of unbootable PCs

  “Microsoft has reports of customers with some AMD devices getting into an unbootable state after installing recent Windows operating system security updates,” says a Microsoft spokesperson. “After investigating, Microsoft has determined that some AMD chipsets do not conform to the documentation previously provided to Microsoft to develop the Windows operating system mitigations to protect against the chipset vulnerabilities known as Spectre and Meltdown.” See [https://www.theverge.com/2018/1/9/16867068/microsoft-meltdown-spectre-security-updates-amd-pcs-issues](https://www.theverge.com/2018/1/9/16867068/microsoft-meltdown-spectre-security-updates-amd-pcs-issues)

Be sure to install any pending patches on your personal computers as well.

**Caveat #1:** Your AntiVirus on Windows matters… Because installing the Windows patches on computers with certain Antivirus software may cause a “Blue Screen of Death”, Microsoft has created a prerequisite before your computer will install the patches. It must first detect a special registry key to be present. AV vendors are working to upgrade their products and push out not only patches, but this registry key. All campus Windows machines should be using Microsoft’s own AV product which has already pushed out this prereq -- but take note of this for home / personal computers. So before you try to install any Windows patches, also make sure that your AV client is fully up to date as well. Some AV vendors have noted that it may take some time to upgrade their product. See [http://www.zdnet.com/article/windows-meltdown-spectre-fix-how-to-check-if-your-av-is-blocking-microsoft-patch](http://www.zdnet.com/article/windows-meltdown-spectre-fix-how-to-check-if-your-av-is-blocking-microsoft-patch) for an overview of the major AV products out there.

**Caveat #2:** If your computer has an AMD logo on the front instead of the Intel Inside logo, you might want to wait a few days before installing the Windows OS patches, see [http://www.eweek.com/security/microsoft-investigating-problematic-meltdown-patch-on-amd-pcs](http://www.eweek.com/security/microsoft-investigating-problematic-meltdown-patch-on-amd-pcs)

• Linux is currently a waiting game...
- RedHat Enterprise Linux -- “We expect all packages for RHEL7 to be available shortly, with RHEL6 following closely behind.” Once available, we’ll push the patches out to all campus RHEL workstations. Details: https://access.redhat.com/articles/3307751
- Ubuntu Linux -- No patches yet, but they’re being worked on. Will be released to campus machines once available. Details: https://wiki.ubuntu.com/SecurityTeam/KnowledgeBase/SpectreAndMeltdown

BIOS Upgrades are the final part of the solution -- also the most difficult to install en masse, and the most impacted by who made your computer and the age of the computer.

Hardware vendors are scrambling to create BIOS patches for their many model lines. This isn’t a particularly fast process, so they’re focused on their newest models and working their way backwards.

There is the chance that some vendors simply won’t create BIOS upgrades for models they no longer actively support. Microsoft has made this decision on its earliest Surface tablets. Dell has released or announced BIOS patches for many of its more recent model lines, but we’ve not yet heard about older models lines (of which we have hundreds of in production).

In CAAT, we will be working out ways to upgrade our NCSU systems, but you should go see what your personal machine’s vendors are saying. Here’s some links for the main vendors.
- Apple: A special case as they’ll patch the BIOS on their machines during the OS patch process. So just install those patches as soon as you see you have some pending.

===== CAAT will be working to update our computers for the next couple months to address this fiasco. At this time, there are no known exploits so while its important that we patch our computers, it’s not an immediate threat. And as I’ve noted, not all of the upgrades that we’ll need for BIOS, OS, or even browsers have been released yet.

So patch your machines as usual (and reboot), see if your computer’s manufacturer has a new BIOS for you, but don’t lose any sleep over this just yet.

Additional Information:
https://security.ias.edu/what-im-doing-about-meltdown-and-spectre