Volume 1, No. 3 | May–June 2018

RAIL

The Journal of Robotics, Artificial Intelligence & Law

fastcase FULL COURT PRESS

RAIL
The Journal of Robotics, Artificial Intelligence & Law
Volume 1, No. 3 | May–June 2018

THE JOURNAL OF ROBOTICS, ARTIFICIAL INTELLIGENCE & LAW (ISSN 2575-5633 (print) /ISSN 2575-5617 (online) at $495.00 annually is published six times per year by Full Court Press, a Fastcase, Inc., imprint. For customer support, please contact Fastcase, Inc., 711 D St. NW, Suite 200, Washington, D.C. 20004, 202.999.4777 (phone), 202.521.3462 (fax), or email customer service at support@fastcase.com.

Publishing Staff
Publisher: Morgan Morrissette Wright
Journal Designer: Sharon D. Ray
Cover Art Design: Juan Bustamante

Cite this publication as:

The Journal of Robotics, Artificial Intelligence & Law (Fastcase)

A Full Court Press, Fastcase, Inc., Publication

Editorial Office

711 D St. NW, Suite 200, Washington, D.C. 20004
https://www.fastcase.com/

POSTMASTER: Send address changes to THE JOURNAL OF ROBOTICS, ARTIFICIAL INTELLIGENCE & LAW, 711 D St. NW, Suite 200, Washington, D.C. 20004.

Articles and Submissions

Direct editorial inquires and send material for publication to:

Steven A. Meyerowitz, Editor-in-Chief, Meyerowitz Communications Inc., 26910 Grand Central Parkway, #18R, Floral Park, NY 11005, smeyerowitz@meyerowitzcommunications.com, 718.224.2258.

Material for publication is welcomed—articles, decisions, or other items of interest to attorneys and law firms, in-house counsel, corporate compliance officers, government agencies and their counsel, senior business executives, scientists, engineers, and anyone interested in the law governing artificial intelligence and robotics. This publication is designed to be accurate and authoritative, but neither the publisher nor the authors are rendering legal, accounting, or other professional services in this publication. If legal or other expert advice is desired, retain the services of an appropriate professional. The articles and columns reflect only the present considerations and views of the authors and do not necessarily reflect those of the firms or organizations with which they are affiliated, any of the former or present clients of the authors or their firms or organizations, or the editors or publisher.

QUESTIONS ABOUT THIS PUBLICATION?

For questions about the Editorial Content appearing in these volumes or reprint permission, please call:

Morgan Morrissette Wright, Publisher, Full Court Press at mwright@fastcase.com or at 202.999.4878

For questions or Sales and Customer Service:

Customer Service
Available 8am–8pm Eastern Time
866.773.2782 (phone)
support@fastcase.com (email)

Sales
202.999.4777 (phone)
sales@fastcase.com (email)
ISSN 2575-5633 (print)
ISSN 2575-5617 (online)

What Are "Meltdown" and "Spectre" and Why Should a Business Care?

Nicholas R. Merker and Matthew A. Diaz*

The authors of this article discuss the cybersecurity risks associated with "Meltdown" and "Spectre," two hacking techniques that circumvent the security measures in place to protect the raw, unencrypted data during computer processing, and what businesses can do about it.

Recently, many people have been hearing the words "Meltdown," "Spectre," and "cybersecurity risk" spoken in the same sentence. But how worried should you really be? Below is a summary of what you need to know about Meltdown and Spectre and how to proactively protect your computer and data.

When Were the Vulnerabilities Found, and Why Did it Take so Long for Me to Find Out?

It may surprise you to learn the Meltdown and Spectre vulnerabilities were discovered in the summer of 2017.[1] However, it was *not* out of negligence that the tech industry did not inform the public of the issue. Waiting to make these major vulnerabilities public is common practice among the tech industry.[2] This delay allowed the tech companies time to develop patches to address the vulnerabilities. Furthermore, by not making these findings public earlier, the tech industry prevented hackers from learning about the vulnerabilities and exploiting them for malicious or criminal purposes.[3]

What Part of My Computer is Affected?

It is important to highlight that the Meltdown and Spectre vulnerabilities are neither hardware problems with the CPU nor software bugs with an application.[4] Rather, these issues occur at the processor level in how computer instructions are carried out.[5]

Robotics, Artificial Intelligence & Law / May–June 2018, Vol. 1, No. 3, pp. 193–199.

ISSN 2575-5633 (print) /ISSN 2575-5617 (online)

There are "inviolable" spaces in the computing process where data passes through in a raw, unencrypted form.[6] At that level, there are powerful protections in place to prevent this transfer of data from being interfered with or seen by any other processes or applications.[7]

What has happened is researchers have discovered two techniques—Meltdown and Spectre—that circumvent the security measures in place to protect the raw, unencrypted data during processing.[8] This data can include passwords, proprietary information, or encrypted communications.[9]

What Do Meltdown and Spectre Even Mean?

Meltdown primarily affects most Intel processor chips as well as high-performance ARM chips.[10] Meltdown affects the core part of your computer's operating system—the "kernel"—which handles the coordination of data by moving data between different sorts of memory on the chip and elsewhere in the computer.[11] This kernel also segregates and protects memory spaces and prevents applications interfering with other data, as well as prevents malicious software from seeing and modifying the data.[12] The Meltdown vulnerability allows hackers to access the kernel and see the information being transmitted, such as your password or sensitive communications.

Spectre affects chips made by Intel, AMD, and ARM, as well as likely affects every other processor on the market that offers the computing process known as "speculative execution."[13] Effectively, this vulnerability becomes broader than Meltdown by encompassing mobile phones, embedded devices, and essentially anything with a chip, including thermostats and baby monitors.[14] Spectre allows hackers to "trick" applications into disclosing information that is normally protected in a computer's memory by exploiting the speculative execution process.[15] The Spectre vulnerability will essentially leak data that is usually secured and protected.[16]

Why Should I Be Worried?

You need to worry about these threats because they likely affect your computer and devices. In total, Meltdown and Spectre affect

billions of computer systems around the world from mobile phones to desktop computers.[17] The Meltdown vulnerability is said to be "patchable"[18] by building stronger security measures around the kernel, but at a cost—a reduction in your computer's processing speed of anywhere from five percent to as much as 30 percent.[19] The Spectre vulnerability, unfortunately, is not likely to be completely fixed in the near future.[20] Since Spectre targets the speculative computing process of your computer, a patch is harder to develop. Systemic fixes have been developed for some aspects of Spectre, but the only real resolution to the vulnerability would be to completely redesign the chip processor, which would take years.[21]

What Can I Do About It?

Unfortunately, users individually can do very little at this point to avoid these security flaws since they are happening "under the hood" so to speak.[22] However, patches have already been released by Microsoft and Apple, as well as other tech companies to address the Meltdown vulnerability.[23] The Spectre vulnerability, on the other hand, will take time to patch due to its unique vulnerability. Forbes is maintaining a list of patches being released by all the major tech companies in response to Meltdown and Spectre.[24]

The important thing to remember is you should check your computer and devices for any software updates, whether you are an individual user or someone responsible for a major IT network.[25]

What if I Run a Business? What Should My IT Professional Do?

Beyond the installation of the above-mentioned patches, it has become a common business practice to employ something called a "patch management program." If this is the first time you are hearing this phrase, it's time to listen up!

A patch management program is a strategy that businesses and other organizations with sophisticated IT systems use for managing patches or upgrades to software applications and other technologies.[26] A patch management program will include the acquisition, testing, and installation of multiple patches to a computer system.[27] But the program is far more sophisticated than just these tasks.

Fred Avolio in a TechTarget article distilled the patch management process into six general steps:

1. Develop an up-to-date inventory of all production systems (including operating system ("OS") types and versions, internet protocol ("IP") addresses, and other critical items);
2. Devise a plan for standardizing production systems to the same OS version and application software;
3. List all security controls your business has implemented;
4. Compare reported vulnerabilities against the inventory list;
5. Classify any risks and assess the vulnerability and likelihood of a cyber-attack; and
6. Determine which patches to deploy on your network.[28]

There are two ways of implementing a patch management program. It can either be (1) manually administered by an IT professional in your business or (2) automatically managed by installing patch management software. Manual patch management can be an onerous and tedious process. IT professionals must identify, out of the hundreds of patches released every month, which patches must be addressed and subsequently initiate and monitor the more critical updates.[29] What's more, because of the risk of having outdated software and the nature of cyber-threats, this process must be repeated on a weekly basis, if not more frequently.[30]

On the other hand, patch management software automates the process into an easy product for businesses to purchase and install.[31] The greater challenge comes when deciding which patch management software and strategy works best for your business.[32] Patch management software may be a better solution for your business because it enables your business's IT professional to delegate the manual tasks described above to sophisticated software to distribute patches system-wide.[33] Furthermore, patch management software can automatically populate compliance reports, indicating which computers have been updated as well as whether a patch was successful.[34]

For those interested in implementing a patch management system via patch management software, TechTarget provides some important tips on how to select and purchase the right software for your business.[35]

Are There Other Reasons I Should Have a Patch Management Program?

Aside from helping your business prevent a data breach due to vulnerabilities such as Meltdown and Spectre, a patch management program can also help your business comply with various federal and state laws. Focusing on federal law, there are various regulatory frameworks established to ensure that businesses manage, handle, and safeguard the data of U.S. citizens properly. These range from the Health Insurance Portability and Accountability Act ("HIPAA"), which affects many health care providers, to the Gramm-Leach-Bliley Act ("GLBA"), which affects financial institutions. Non-compliance with these and various other laws can result in a regulatory enforcement action, ranging from a civil forfeiture to moratoriums for certain practices.

One particular law that implicates IT management is the Sarbanes-Oxley Act ("SOX"). The SOX is a law that established a number of reforms to "enhance corporate responsibility, enhance financial disclosures, and combat corporate and accounting fraud . . . ."[36] Particularly, Section 404 of the SOX requires that chief executives of publicly traded companies attest to the maintenance of internal controls over the financial reporting processes of the company, including IT systems.[37] Effectively, IT departments must identify system controls and prove to auditors that said controls have been properly implemented, maintained, and monitored to ensure the integrity of financial reporting data.[38] This means that vulnerabilities like Meltdown and Spectre can result in a regulatory enforcement action by the Securities and Exchange Commission against the head of a publicly traded company.

Notes

* Nicholas R. Merker is a partner at Ice Miller LLP and co-chair of the firm's Data Security and Privacy Practice. Matthew A. Diaz is an attorney in the firm's Data Security and Privacy Practice Group. They may be reached at nick.merker@icemiller.com and matthew.diaz@icemiller.com, respectively.

1. Samuel Gibbs, *Meltdown and Spectre: 'worst ever' CPU bugs affect virtually all computers*, Guardian (Jan. 4, 2018), https://www.theguardian.com/technology/2018/jan/04/meltdown-spectre-worst-cpu-bugs-ever-found-affect-computers-intel-processors-security-flaw.

2. Todd Bishop & Tom Krazit, *What are Meltdown and Spectre? GeekWire's guide to the problems with the world's computer chips*,

GeekWire (Jan. 6, 2018), https://www.geekwire.com/2018/meltdown-spectre-geekwires-guide-vulnerabilities-worlds-computer-chips/.

3. *Id.*

4. Devin Coldewey, *Kernel Panic! What are Meltdown and Spectre, the bugs affecting nearly every computer and device*, TechCrunch (Jan. 3, 2017), https://techcrunch.com/2018/01/03/kernel-panic-what-are-meltdown-and-spectre-the-bugs-affecting-nearly-every-computer-and-device/.

5. *Id.*

6. *Id.*

7. *Id.*

8. *Id.*

9. *Id.*

10. Peter Bright, *Meltdown and Spectre: Here's what Intel, Apple, Microsoft, others are doing about it*, ARS Technica (Jan. 5, 2018), https://arstechnica.com/gadgets/2018/01/meltdown-and-spectre-heres-what-intel-apple-microsoft-others-are-doing-about-it/.

11. Chris Maraniuk & Mark Ward, *Meltdown and Spectre: How chip hacks work*, BBC (Jan. 4, 2018), http://www.bbc.com/news/technology-42564461.

12. Devin Coldewey, *Kernel Panic! What are Meltdown and Spectre, the bugs affecting nearly every computer and device*, TechCrunch (Jan. 3, 2017), https://techcrunch.com/2018/01/03/kernel-panic-what-are-meltdown-and-spectre-the-bugs-affecting-nearly-every-computer-and-device/.

13. Peter Bright, *Meltdown and Spectre: Here's what Intel, Apple, Microsoft, others are doing about it*, ARS Technica (Jan. 5, 2018), https://arstechnica.com/gadgets/2018/01/meltdown-and-spectre-heres-what-intel-apple-microsoft-others-are-doing-about-it/.

14. Devin Coldewey, *Kernel Panic! What are Meltdown and Spectre, the bugs affecting nearly every computer and device*, TechCrunch (Jan. 3, 2017), https://techcrunch.com/2018/01/03/kernel-panic-what-are-meltdown-and-spectre-the-bugs-affecting-nearly-every-computer-and-device/.

15. *Id.*

16. Chris Maraniuk & Mark Ward, *Meltdown and Spectre: How chip hacks work*, BBC (Jan. 4, 2018), http://www.bbc.com/news/technology-42564461.

17. *Id.*

18. Todd Bishop & Tom Krazit, *What are Meltdown and Spectre? GeekWire's guide to the problems with the world's computer chips*, GeekWire (Jan. 6, 2018), https://www.geekwire.com/2018/meltdown-spectre-geekwires-guide-vulnerabilities-worlds-computer-chips/.

19. Devin Coldewey, *Kernel Panic! What are Meltdown and Spectre, the bugs affecting nearly every computer and device*, TechCrunch (Jan. 3, 2017), https://techcrunch.com/2018/01/03/kernel-panic-what-are-meltdown-and-spectre-the-bugs-affecting-nearly-every-computer-and-device/.

20. *Id.*

21. *Id.*

22. Samuel Gibbs, *Meltdown and Spectre: 'worst ever' CPU bugs affect virtually all computers*, Guardian (Jan. 4, 2018), https://www.theguardian.com/technology/2018/jan/04/meltdown-spectre-worst-cpu-bugs-ever-found-affect-computers-intel-processors-security-flaw.

23. Chris Maraniuk & Mark Ward, *Meltdown and Spectre: How chip hacks work*, BBC (Jan. 4, 2018), http://www.bbc.com/news/technology-42564461.

24. Thomas Fox-Brewster, *Here Are All the Available Fixes You Need for Those Huge Chip Backs—UPDATED*, Forbes (Jan. 4, 2018), https://www.forbes.com/sites/thomasbrewster/2018/01/04/google-microsoft-apple-updates-for-meltdown-spectre-intel-processor-vulnerabilities/#5295f5445c31.

25. Todd Bishop & Tom Krazit, *What are Meltdown and Spectre? GeekWire's guide to the problems with the world's computer chips*, GeekWire (Jan. 6, 2018), https://www.geekwire.com/2018/meltdown-spectre-geekwires-guide-vulnerabilities-worlds-computer-chips/.

26. *Patch Management*, techopedia, https://www.techopedia.com/definition/13835/patch-management.

27. *Patch Management*, TechTarget, http://searchenterprisedesktop.techtarget.com/definition/patch-management.

28. Fred Avolio, *Six steps for security patch management best practices*, TechTarget, http://searchsecurity.techtarget.com/Six-steps-for-security-patch-management-best-practices.

29. *Select the best patch management software for your company*, TechTarget, http://searchsecurity.techtarget.com/buyersguide/Select-the-best-patch-management-software-for-your-company#guideSection1.

30. *Id.*

31. *Id.*

32. *Id.*

33. Earl Follis, *Introduction to automated enterprise patch management software*, TechTarget, http://searchsecurity.techtarget.com/feature/Introduction-to-automated-patch-management-products-in-the-enterprise.

34. *Id.*

35. *Select the best patch management software for your company*, TechTarget, http://searchsecurity.techtarget.com/buyersguide/Select-the-best-patch-management-software-for-your-company#guideSection1.

36. *The Laws That Govern the Securities Industry*, U.S. Sec. & Exch. Comm'n, https://www.sec.gov/answers/about-lawsshtml.html#sox2002.

37. Global Technology Audit Guide, Change and Patch Management Controls: Critical for Organizational Success 8 (2012), https://chapters.theiia.org/montreal/ChapterDocuments/GTAG%202%20-%20Change%20and%20Patch%20Management%20Controls%20Critical%20for%20Organizational%20Success_2nd%20ed.pdf; *Solution Brief—Comply with Sarbanes-Oxley (SOX)*, Elemental, https://www.elementalsecurity.com/alldocs/E_Sarbanes.php.

38. Solution Brief—Comply with Sarbanes-Oxley (SOX), ELEMENTAL, https://www.elementalsecurity.com/alldocs/E_Sarbanes.php.