Spectre en Meltdown

Rein de Jong

Wat is het en wat doen we eraan?

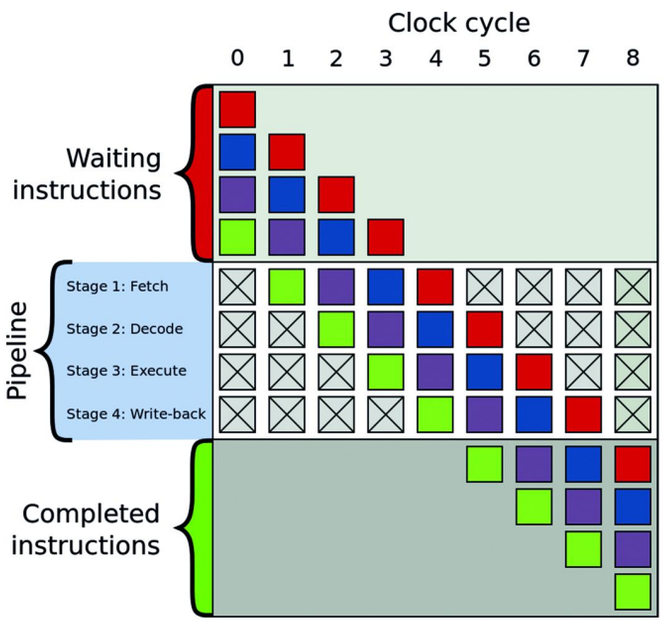
De wereld wordt sinds begin 2018 opgeschrikt door meldingen van allerlei kwetsbaarheden in digitale apparatuur. Mensen zoals jij en ik vrezen de greep op essentiële zaken te verliezen. De vragen die we ons moeten stellen, zijn: 'Kunnen we straks nog wel wereldwijd communiceren? Kunnen we nog betalen? Zijn onze gegevens nog wel veilig? Zijn wij nog wel veilig? Wat als het internet stopt met werken?' Heb je daar al eens over nagedacht? Niet? Misschien wijs om dat op een rustig moment toch even te doen! Ik ben tot de conclusie gekomen dat er ook positieve elementen te ontdekken zijn aan een internetloos tijdperk. Alleen wil ik dat nu niet uitproberen.

Criminelen, overheden en bedrijven maken gebruik van fouten in menselijke ontwerpen. Dachten wij nog dat er alleen maar fouten zaten in het besturingssysteem en de software, dan hebben wij dat mis! Er wordt ook gebruik gemaakt van fouten in het ontwerp van netwerken – denk aan de DDoS-aanvallen van de laatste tijd – en de verbindingsopbouw in het net (DNS). Onderschat je eigen rol ook niet. De gebruiker staat zelf aan de basis van veel ellende door achteloosheid, waar anderen met behulp van 'social engineering' dankbaar misbruik van maken.
Onlangs zijn er twee ontwerpfouten ontdekt in de hardware van digitale apparatuur. Die twee zwakke plekken, Meltdown en Spectre, betreffen de wijze waarop processoren met het geheugen omgaan. Niet alleen de klassieke computer is kwetsbaar, maar ook telefoons en tablets die van bepaalde chipsets gebruik maken. Meltdown raakt alleen Intelchips; Spectre gaat nog veel verder en treft bijna elke processor. Het probleem zit in de architectuur zelf!

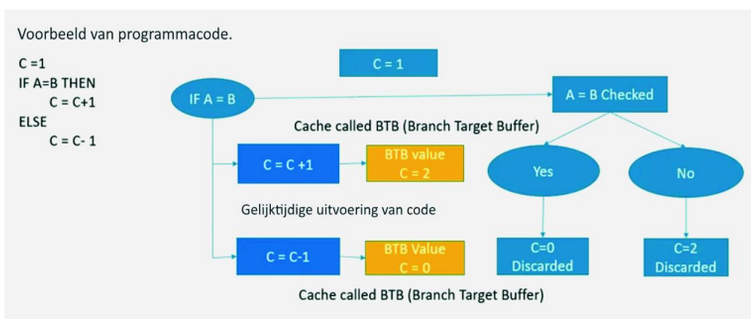
Wat is het?

Beide fouten manifesteren zich, al sinds 1995, in de basis van processoren. Deze basis wordt de kernel genoemd. In de kernel wordt alle data in zijn pure vorm verwerkt zonder enige vorm van afscherming. Daarom wordt de kernel op een hoger niveau afgeschermd van de applicaties die op het systeem draaien. Het wordt toepassingsprogramma's niet toegestaan om data van andere processen te lezen.
Primair zit het probleem in het gebruik van de geheugencache. De daarin vastgelegde data kan onrechtmatig worden gelezen. In de kernel wordt geheugen - kernel space - gebruikt om gegevens op te slaan en te bewerken. De uitwisseling van die data kan, door de fouten in het ontwerp, worden afgevangen door een kwaadwillend programma dat alleen maar het eigen geheugengebied mag gebruiken - user space -. Daarmee wordt het verbod tot het lezen van elkaars data - user space - omzeild. Gevoelige gegevens kunnen dan uit het geheugengebied van een ander programma worden gevist. Denk daarbij aan de wachtwoorden opgeslagen in een password-manager of de browser, je persoonlijke mail, foto's en andere waardevolle gegevens. De kernel space is niet meer veilig!

De kwetsbaarheid zit in de algemeen gebruikte processorarchitectuur en kan daardoor misbruikt worden bij de processoren van Intel, AMD, ARM, IBM en Sun.
Al deze processoren gebruiken *'speculatieve uitvoering'*; dat wil zeggen: in plaats van te wachten op een volgende instructie, wordt alvast vooruit gedacht over de uitvoering van de volgende instructies. Als er goed gegokt is, wordt dat resultaat gebruikt en is het proces versneld. Zo niet, dan wordt het voorspelde resultaat weggegooid.



Alle instructies worden voorzien van privileges (gebruiksrechten) waardoor vooraf wordt bepaald wat wel en wat niet mag. Juist de instructies van speculatieve uitvoering worden NIET vooraf, maar pas wanneer zeker is dat die gebruikt gaan worden, dus na executie, getest op privileges. Dat geeft de speculatieve instructie toegang tot alle geheugengebieden inclusief kernel space. Het wordt uiteindelijk wel gestopt. Daarom is het in principe geen probleem. Echter, een slim programmaatje kan inzien wat de speculatieve instructie kon zien. Dit is een simpele verwoording van een complex proces[1].



Wat zijn de verschillen tussen Meltdown en Spectre?
Meltdown verbreekt de fundamentele isolatie tussen het besturingssysteem (kernel space) en gebruikerstoepassingen (user space) waardoor het geheugengebieden kan lezen die ontoegankelijk zouden moeten zijn. Alleen Intel heeft hier last van omdat Intel als enige de privileges van de speculatieve instructies pas achteraf test.

Van **Spectre** bestaan twee varianten, die de grenzen tussen gebruikersapplicaties kunnen overschrijden. Het staat de aanvaller toe om programma's te verleiden hun geheimen te

lekken. Juist de programma's die veiligheid goed geregeld hebben zijn kwetsbaarder doordat ze extra controles uitvoeren. Al die extra controles bieden handvatten die het aanvalsgebied van de malware vergroten. Deze kwetsbaarheid treft alle fabrikanten.
De kwetsbaarheid van Spectre is moeilijker te benutten dan die van Meltdown, maar is ook minder eenvoudig te verhelpen.

Is het erg?

Eenvoudigweg: **Ja!** De diverse patches om de kwetsbaarheid te verminderen kunnen de systeemperformance vertragen. Hoe ouder de architectuur, des te groter de impact. Op zich zal het misbruiken van de kwetsbaarheid wel meevallen omdat de aanvaller eerst toegang moet krijgen tot het aan te vallen systeem. Ben je voorzichtig, download je alleen uit betrouwbare bron, en ben je terughoudend met mail uit onbekende hoek, dan is de kans op zo'n besmetting niet groot.
Voor Meltdown komen algemene patches. Het is mogelijk om voor specifieke Spectre-aanvallen patches te maken. Aan die patches wordt gewerkt.
In het bijzonder zijn Cloud-providers zoals Amazon, IBM en Microsoft Azure, kwetsbaar omdat zij op hun systemen processen van verschillende klanten draaien op dezelfde hardware. De software van een persoon kan, in theorie, spioneren naar de gegevens van andere klanten; ook wanneer die processen draaien in verschillende virtuele omgevingen. De onderliggende hardware is immers de toegangspoort. Al die grote organisaties geven aan dat hun systemen actief worden of zijn gepatcht. Ik betwijfel of dat ook voor Spectre geldt. Wel is het zo dat de grote jongens korte lijntjes met de fabrikanten hebben. Reken maar dat zij, ten koste van veel rekenkracht, de BIOS-updates het eerst krijgen.

Hoe kun je zien of je kwetsbaar bent en waarvoor?

Je bent bijna zeker kwetsbaar! Voor Meltdown zijn er inmiddels patches voor de meeste systemen. Voor Spectre zijn er nog weinig patches bekend. De bekende Steve Gibson, IT-security-goeroe, heeft op zijn site een programma, InSpectre[2] voor Windows ter beschikking gesteld. Daarmee kun je eenvoudig testen of je al dan niet kwetsbaar bent voor Meltdown en Spectre en welke impact dat heeft op de snelheid van het systeem.
Er zijn meerdere tools te vinden die ook de kwetsbaarheid kunnen testen. Van InSpectre weet ik zeker dat het van een veilige bron komt.

Wat kun je doen?

Kijk of er updates zijn voor je Intel-processor (UEFI/BIOS- en firmware-updates). Intel geeft aan dat zij voor processoren van de laatste vijf jaar microcode-updates ter beschikking hebben[3]. Oudere processoren volgen mogelijk later. Vervolgens zullen er door de moederbordfabrikanten BIOS-updates moeten worden verzorgd. Bezoek de website van je computer- en/of moederbordfabrikant en installeer de laatste updates[4]. Updates vanaf december 2017 bevatten de relevante patches.
Update naar de laatste versie van je OS en installeer de laatste beveiligingsupdates. Wanneer je dit te snel doet, loop je de kans dat je tegen ongewenste effecten aanloopt zoals met de eerste patches van Intel die onverwachte reboots en opstartproblemen veroorzaakten. Wacht dus een of twee weken. Op het moment dat ik dit schrijf, begin maart 2018, is het volgende bekend:

1. *Windows*
   Microsoft heeft inmiddels een patch uitgebracht die je beschermt tegen Meltdown. Deze is eenvoudig via Windows Update te installeren, of is al geïnstalleerd omdat die automatisch wordt uitgerold.
2. *Linux*
   Verschillende distributies hebben kernel-updates uitgebracht waarmee de kwetsbaarheden verholpen worden.
3. *Android*
   Begin januari is er een beveiligingsupdate beschikbaar gekomen. De Nexus- en Google-apparaten hebben de update inmiddels. Wanneer die voor andere apparaten beschikbaar komt, is fabrikantafhankelijk. Kijk regelmatig in de instellingen van de telefoon of er een update beschikbaar is. Daar kun je ook zien of je een update van na 5 januari hebt ontvangen. Waarschijnlijk ben je dan veilig. Helaas worden niet alle Android apparaten voorzien van een update. Welke apparaten? Dat zie je hier[5].
4. *Apple*
   HighSierra 10.13.2 is inmiddels voorzien van een patch die Meltdown moet tegengaan. Er is onduidelijkheid over de patches voor Sierra en El Capitan. iOS 11.2.2 is inmiddels gepatcht en ook tvOS 11.2 is beschermd. Voor Spectre worden later updates verwacht.
   Je kunt in de Apple-store controleren op de updates. Meer info6.
5. *Chrome OS*
   Vanaf versie 63 Chrome OS zijn er patches aangebracht tegen Meltdown en Spectre. Controleren op updates kun je bij 'Over Chrome OS' in de instellingen.
6. *Overige*
   De in de Raspberry Pi gebruikte ARM-chips zijn volgens de makers niet kwetsbaar[7].
   Voor andere apparaten: zoek naar de relevante informatie op het internet.
   Zoekwoorden: Spectre Meltdown +<Fabrikant> ~patch OR ~update OR ~kwetsbaarheid
   Voor <Fabrikant> Zou je in kunnen vullen: Intel, Amazon, TransIP, KPN, o.i.d.
7. *Antivirus*
   Er is een aantal antivirusproducten dat zelf gebruik maakt van niet-gesupporte kernelfuncties. Microsoft heeft alle antivirus-fabrikanten gesommeerd een registersleutel aan te brengen[8] als teken dat hun software compatible is met de laatste veiligheidsupdates van Microsoft. Is die sleutel er niet, dan worden de updates uitgesteld. Gelukkig hebben de meeste antivirusproducten inmiddels al voorzieningen om de kwetsbaarheden tegen te gaan. Kijk dus of er voor jouw antivirusproduct updates zijn. Kijk daarvoor in de interface van je antivirusprogramma. Uiteraard is Windows Defender hier al op aangepast.

Welke browsers beschermen je en per wanneer?

Omdat, in het slechtste geval, Javascriptcode, die in de browser wordt uitgevoerd, geheugen kan lezen, zou het geen toegang moeten hebben tot kwetsbare gegevens van andere processen. Daarom zijn de ontwikkelaars van browsers hard bezig om de verschillende sites van elkaar te isoleren. Google Chrome (versie 64) heeft dat al voor elkaar, mits je 'Site Isolation' activeert[9].

Mozilla heeft snel een aantal patches voor FireFox gemaakt. Microsoft heeft Edge en Internet Explorer beveiligd. Ook Opera en Safari melden dat ze veiligheidsupdates voor hun browsers hebben gemaakt. Zelf kun je ook maatregelen nemen door Javascript standaard uit te schakelen en selectief te activeren voor betrouwbaar geachte sites. Kijk bijvoorbeeld naar de extensie NoScript.
Performanceverlies door de patch zoveel mogelijk beperken? Zeker bij iets oudere processoren, - Haswell en ouder- en vooral wanneer je nog Windows 7 of 8 draait, is de invloed aanmerkelijk. De eerste tests wijzen op een mogelijke achteruitgang van processorprestaties van tien procent of meer. Nieuwere pc's zullen er daarentegen nauwelijks iets van merken.

Wat je ook doet, wees wijs en verwijder de patches niet, want de aanvallen die met Meltdown en Spectre kunnen worden uitgevoerd hebben grote consequenties.

Dat betekent echter niet dat je de vertraging maar lijdzaam moet ondergaan

Wat kun je doen?

Upgrade naar de laatste versie van Windows 10
De door Microsoft uitgerolde patches voor Windows 10 (1709) hebben minder invloed dan die voor Windows 7 en 8 en zelfs voor de oudere versies van Windows 10. Op vergelijkbare hardware zal Windows 10 beter presteren dan Windows 7 en 8 omdat beide laatste meer overgangen tussen user en kernel mode bevatten. Windows 10 is wat de programmacode betreft beter toegerust en geoptimaliseerd, omdat die overgangen tot een minimum zijn teruggebracht.
Begin maart 2018 meldt Microsoft dat het de microcode-update van Intel tegen de tweede variant van Spectre gaat verspreiden via Windows Update naar de systemen met Windows 10 (1709). Het betreft een microcode-update voor systemen met een bepaalde Intel Skylake-processor[10]. Deze update dient handmatig te worden aangebracht. Ik adviseer echter om regelmatig de fabrikanten-website van je systeem of moederbord te raadplegen op BIOS-updates voor Meltdown en Spectre. Een BIOS-update is een beter alternatief voor een update van het besturingssysteem.

Upgrade je hardware

Mocht je niet kunt wachten totdat er veilige CPU's verschijnen (2019?) en kun je zelf je moederbord vervangen, dan zou je kunnen overwegen om te upgraden naar een nieuwer moederbord en processor van de nieuwste generatie (Skylake, Kabylake of nieuwer). Alles vanaf het jaar 2017 wordt minder door de patches geplaagd dan de hardware van daarvoor. Intel heeft een persbericht uitgebracht waarin zij aangeven te verwachten al in 2018 op de markt te komen met aangepaste chips die de kwetsbaarheden niet meer bevatten. Dat worden aangepaste modellen van actuele chips. Dus nog geen nieuw ontwerp. Daarvoor moet je naar verwachting minimaal twee jaar geduld hebben.
Dat neemt niet weg dat er voor recente processoren van de Skylake-familie veel eerder patches komen, of er al zijn, dan voor de oudere processorseries. Ook zal het performanceverlies minimaal zijn.

Verwijder de beveiliging in het register

Windows staat je toe de beveiliging te verwijderen uit het register. Dit maakt je systeem kwetsbaar voor Meltdown en Spectre. Dat is alleen te overwegen wanneer je maar een beperkt aantal toepassingen uit een veilige bron uitvoert of een server draait met een beperkt aantal veilige toepassingen.
Ik raad het echter sterk af. Je bent niet alleen een gevaar voor jezelf, maar ook voor anderen. Jouw systeem kan zomaar een aanvalsbasis worden met nog meer ellende tot gevolg. Vergelijk het maar met het bewust rijden in een auto met slechte remmen. Zelf denk je er rekening mee te houden, maar …

De tool InSpectre[2] laat je deze wijziging in het register doorvoeren. Voordat je definitief besluit om de beveiliging te omzeilen, test dan eerst de performance van je pc met een tooltje zoals UserBenchmark. Maar test het vooral met je eigen applicaties. Voelen die echt trager aan? Kun je er al dan niet mee leven?

Tot slot

De architectuur van de huidige moderne processoren zal danig op zijn kop moeten om deze kwetsbaarheden het hoofd te kunnen bieden. Dus wanneer je de aanschaf van een nieuwe computer, smart-device of IoT-apparaat kunt uitstellen, heb je daar nu een extra argument voor.

Links en bronnen:

1. Speculatieve uitvoering	http://bit.ly/specex
2. Test op kwetsbaarheid	http://bit.ly/r-inspectre
3. Intel-statement	http://bit.ly/r-chintel
4. Bios-updates	http://bit.ly/r-bbios
5. Android-updates	http://bit.ly/r-chandr http://bit.ly/r-chandr2
6. Apple-updates	http://bit.ly/r-chapple
7. Raspberry Pi	http://bit.ly/r-chrasp
8. Antivirus	http://bit.ly/r-chav
9. Site Isolation	http://bit.ly/r-sitis
10. Intel-updates	http://bit.ly/r-mcu-intel
Tweakers	http://bit.ly/r-twms3w
Filmpje Spec. uitvoering	http://bit.ly/r-pms