Sicherheitslücke in allen aktuellen Prozessoren

Meltdown und *Spectre*

Kurs IT Sicherheit
Prof. Dipl.-Ing. Klaus Knopper
Januar 2018

1 In the News

- https://www.heise.de/security/meldung/Massive-Luecke-in-Intel-CPUs-erfordert-umfassende-Patches-3931562.html
- https://www.heise.de/security/meldung/Gravierende-Prozessor-Sicherheitsluecke-Nicht-nur-Intel-CPUs-betroffen-erste-Details-und-Updates-3932573.html
- https://www.heise.de/mac-and-i/meldung/Meltdown-und-Spectre-Alle-Macs-und-iOS-Geraete-betroffen-3934477.html
- https://www.heise.de/newsticker/meldung/Prozessorluecke-Auch-Qualcomm-CPUs-sind-anfaellig-3935270.html
- https://www.heise.de/newsticker/meldung/AMD-rudert-zurueck-Prozessoren-doch-von-Spectre-2-betroffen-Microcode-Updates-fuer-Ryzen-und-Epyc-in-3939975.html

2 Was ist wirklich das Problem?

- https://security.googleblog.com/2018/01/todays-cpu-vulnerability-what-you-need.html
- https://en.wikipedia.org/wiki/Speculative_execution#Security_vulnerabilities

2.1 Hintergrund: Virtual Memory, Process Scheduler

Moderne Prozessoren und Betriebssysteme sorgen mit Hilfe der Memory Managing Unit (MMU) dafür, dass jeder Prozess im System nur seinen eigenen Speicherbereich „sieht“, und nicht auf Speicher anderer Programme zugreifen kann. Dies ist ein essentieller Teil des „Virtual Memory“ Konzepts, das aus Hauptspeicher (RAM) und Auslagerungsspeicher auf Festplatte (Swap) einen scheinbar kontinuierlichen Speicher erzeugt, für den es über eine „Address Translation Table“ die dynamische Zuweisung an Systemresourcen gibt, die normalerweise auch nicht durch Programme „umgangen“ werden kann. Der Scheduler (Timer-Baustein im Chipset in Kombination mit Prozess-Management im Betriebssystem-Kern) kümmert sich um die Zuweisung und Wegnahme von Prozessorleistung, Speicher und Hardware-Zugriffen unter Beachtung von Zugriffsrechten. Der CPU-Cache wird zwar von allen Programmen verwendet, um häufig verwendete Programmteile sofort zugreifbar innerhalb der CPU zu halten, aber die Programmierung der Logik soll dafür

sorgen, dass auch die im CPU-Cache gehaltenen Programmteile „per Programm“ voneinander strikt isoliert bleiben.

In Zusammenhang mit im Chipset programmierten Optimierungen, Out-Of-Order Execution und Speculative Execution existiert hier ein Fehler in der Hardware-Logik, der bei bestimmten Programmabläufen einen Zugriff auf „nicht mehr gebrauchte Daten“ anderer Prozesse zulässt.

https://de.wikipedia.org/wiki/Out-of-order_execution

https://de.wikipedia.org/wiki/Speculative_execution

2.2 Was kann durch die Sicherheitslücke passieren? (User Experience Ebene)

Parallel auf dem System laufende, entsprechend (bösartig) programmierte Programme können Speicher anderer Programme auslesen, und z.B. Passwörter, Zugangs-Daten, Bitcoins, … stehlen, auf die sie über das Auslesen von Speicherbereichen anderer Programme durch den CPU-Fehler Zugriff erhalten. Der Benutzer kann dies durch KEINE der gängigen Sicherheitsmechanismen aller Betriebssysteme VERHINDERN.

Sogar aus einer virtuellen Maschine heraus der Zugriff auf Speicher des Hostsystems – auch den anderer virtueller Maschinen – möglich.

Apps auf Smartphones und Tablets können bei entsprechender Programmierung Daten von anderen Apps ausspionieren, auch wenn keine entsprechenden Rechte bei der Installation gesetzt wurden.

2.3 Betroffene CPUs und CVEs

Hersteller	Betroffene CPUs	Variante 1 (CVE-2017-5753) (Spectre)	Variante 2 (CVE-2017-5715) (Spectre)	Variante 3 (CVE-2017-5754) (Meltdown)	Informationen beim Hersteller
AMD	Bislang keine Details bekannt.	Ja	(bislang nicht betroffen, laut AMD *"near-zeor-risk"*)	(nicht betroffen)[4]	[1]
ARM	Cortex	Ja	Ja	Ja	[2]
Intel	CPUs mit Out-Of-Order Execution (CPUs seit 1995, ausgenommen Itanium und Intel Atom vor 2013)	Ja (siehe INTEL-OSS-10002)	Ja (siehe INTEL-SA-00088)	Ja (siehe INTEL-OSS-10003)	[3]

Quelle: *https://www.thomas-krenn.com/de/wiki/Sicherheitshinweise_zu_Meltdown_und_Spectre#Betroffene_Systeme*

2.4 Technische Analyse und Exploits

2.4.1 Meltdown

Meltdown ist eine Hardware-Sicherheitslücke in Mikroprozessoren, über die ein unautorisierter Zugriff auf den Speicher fremder Prozesse möglich ist.

→ https://de.wikipedia.org/wiki/Meltdown_(Sicherheitsl%C3%BCcke)

CVE-Beschreibungen:

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-5754

2.4.2 Spectre

Spectre beschreibt ein Angriffs-Szenario, bei dem Prozessedurch Sicherheitslücken in Mikroprozessoren mit Out-of-order execution Informationen des virtuellen Speichers anderer Prozesse, auf den sie normalerweise keinen Zugriff haben, auslesen können.

→ https://de.wikipedia.org/wiki/Spectre_(Sicherheitsl%C3%BCcke)

CVE-Beschreibungen:

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-5715

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-5753

3 Lösungsansätze

Da der **Hardware-Fehler** der CPU **durch Software nicht reparierbar ist (!)**, müssen die Kern-Konzepte der Betriebssysteme und der CPU-Firmware (Microcode) überarbeitet werden, um Workarounds zu schaffen. Der Fehler wird dadurch zwar nicht eliminiert, aber die Ausnutzung der Sicherheitslücken durch Schadcode wird zumindest erschwert, auf Kosten der System-Performance.

3.1 CPU Microcode (Firmware Ebene)

http://www.zdnet.de/88322397/nur-microcode-updates-koennen-meltdown-und-spectre-lindern

3.2 Betriebssystem (System Ebene)

Statt sich auf die im Prozessor integrierte Memory Managing Unit zu verlassen, werden neue Strategien auf Betriebssystem-Ebene implementiert, z.B. durch *Memory Page Isolation* (Page Tables „per Prozess“ und nicht mehr eine globale Translation Table), dadurch auch härtere Trennung von „Kernel Memory“ und „User Process Memory“

Dadurch bedingt ist ein höherer Overhead in der Speicherverwaltung, in ALLEN Betriebssystemen. In sehr Task-Switching-intensiven Anwendungen wurden bis zu 30% (!) Leistungsverlust gemessen, was auf das ständige Wechseln zwischen den Page Translation Tables und entsprechende Auslastung von Cache und Memory Manegement zurückzuführen ist. Für ein End-User Desktop-System, in dem das I/O-System die höchste Latenz verursacht (z.B. auch mobile OS wie Android), wird (Linux-Kernel) lediglich von einem Performance-Verlust unter 1% ausgegangen, bei manchen Computerspielen und hoch ausgelasteten Servern ist die Performance hingegen deutlicher eingeschränkt (s. Nächster Abschnitt).

4 Probleme mit den Lösungsansätzen

Nach einem „Patch“ von Betriebssystem und Microcode sind Mechanismen installiert, die die Hardware-Sicherheitslücken unter Verlust von früher möglichen Optimierungen zu umgehen versuchen.

1. Performance-Verlust gerade bei rechenintensiven parallelen Anwendungen und vielen parallel laufenden Tasks (z.B. Game-Server).
2. Einige Programme, wie Viren-Scanner diverser Anbieter, scheinen das Auslesen von Speicher, der ihnen nicht „gehört“, als „Feature“ für Speicher-Untersuchungen zu verwenden, und starten nicht mehr. Hierzu zählen einige bekannte Virenscanner!

https://www.heise.de/security/meldung/Meltdown-und-Spectre-Update-fuer-Windows-10-legt-einige-PCs-lahm-3935460.html

https://www.heise.de/newsticker/meldung/Meltdown-und-Spectre-Erste-Klagen-gegen-Intel-Performanceprobleme-kochen-hoch-3935493.html

https://www.heise.de/newsticker/meldung/Meltdown-und-Spectre-Spontane-Neustarts-nach-Updates-von-Intels-Haswell-und-Broadwell-CPUs-3940326.html

https://www.heise.de/newsticker/meldung/Intel-Benchmarks-zu-Meltdown-Spectre-Performance-sackt-um-bis-zu-10-Prozent-ab-SSD-I-O-deutlich-mehr-3938747.html

5 Zusammenfassung/FAQ zu Meltdown/Spectre

https://www.heise.de/newsticker/meldung/FAQ-zu-Meltdown-und-Spectre-Was-ist-passiert-bin-ich-betroffen-wie-kann-ich-mich-schuetzen-3938146.html

6 Nachtrag: Tests

Firefox / Chromium (Javascript-basiert): http://xlab.tencent.com/special/spectre/spectre_check.html

Spectre/Meltdown Check für Linux: https://github.com/speed47/spectre-meltdown-checker
(Besonders interessant: Nur ein Shell-Skript, das bestimmte Signaturen in Kernel und Microcode sucht, kein Exploit)

Spectre/Meltdown Check für Windows (Microsoft): https://support.microsoft.com/en-us/help/4073119/protect-against-speculative-execution-side-channel-vulnerabilities-in