Bijna alle smartphones en laptops onveilig

Bard van de Weijer
Amsterdam

Volgens onderzoekers van de VU zijn vrijwel alle computergeheugens ter wereld onveilig. De techwereld lijkt het probleem echter niet te willen aanpakken.

Het gaat om de geheugens van de drie grote fabrikanten: Samsung, Hynix en Micron, die gezamenlijk 95 procent van de wereldmarkt in handen hebben. Elk type computer is kwetsbaar: van laptops tot smartphones en servers.

De kern van het probleem zit letterlijk ingebakken in het computergeheugen. Het komt erop neer dat de kleinste deeltjes informatie (een bit) zo dicht opeengepakt zitten, dat ze elkaar beïnvloeden. Dit fenomeen wordt een bitflip genoemd. Het kan bewust worden uitgelokt door aanpalende geheugenrijen in korte tijd duizenden keren uit te lezen. Deze uitgelezen enen en nullen leiden dan tot bitflips in het aangrenzende geheugengebied. Daarmee wordt een deel van het geheugen overschreven.

Gevaarlijk wordt het wanneer dit een beveiligd deel van het geheugen is, dat niet toegankelijk hoort te zijn voor onbevoegden. Bijvoorbeeld omdat er een cryptografische sleutel is opgeslagen, of omdat het een afgeschermd deel van het besturingssysteem betreft.

> **De grote vraag is: wisten de fabrikanten dit?**

'Dit is zeer zorgelijk', zegt Herbert Bos, hoogleraar Systems and Network Security aan de VU. 'Als het fundament faalt, is alles wat je daarop bouwt ook in gevaar.'

Rowhammer

Deze techniek om het computergeheugen te kraken staat sinds 2012 bekend als rowhammer ('rijenhamer'). Een belangrijk verschil met andere hacks is dat die meestal zijn gebaseerd op softwarefouten. Maar doordat rowhammer 'ingebakken' zit in de hardware, raakt alle software die erop draait ook gecorrumpeerd. Herstel is niet of nauwelijks mogelijk met software-aanpassingen.

Inmiddels zeggen fabrikanten het probleem te hebben opgelost. Maar dat is volgens de VU-onderzoekers allerminst het geval.

Inderdaad, zegt Bos, de oude truc werkt niet meer. Wie nu probeert geheugens te forceren door telkens naastgelegen geheugenrijen aan te vallen, zal een halt worden toegeroepen.

Maar, ontdekten de VU-onderzoekers, de blokkering kan worden omzeild door eerst de rij ernaast aan te vallen, vervolgens rijen telkens een stukje verderop en dan de bewuste rij opnieuw. Het systeem houdt namelijk in een soort kasboekje bij welke geheugenplekken worden gebruikt. Maar het geheugen hiervan is te klein om heel veel rijen bij te houden. Een paar pogingen verder is het bewakingssysteem 'vergeten' dat de eerste, kwetsbare rij al eens was geprobeerd.

In hun pogingen steeds grotere geheugens te maken, hebben fabrikanten het probleem bovendien verergerd. Ze persen steeds meer transistors op hetzelfde oppervlak. Doordat die dichter op elkaar zitten, lekken ze sneller informatie. 'Waren voorheen 130 duizend pogingen nodig voor een bitflip, nu gaat dat al in 20 duizend keer', zegt assistent-hoogleraar en mede-onderzoeker Kaveh Razavi.

Techwereld

De grote vraag is: wisten de fabrikanten dit? 'Als ze het niet wisten, waren ze naïef', aldus Bos. 'En als ze het wel wisten, liegen ze dat hun geheugens veilig zijn.' Het lijkt me waarschijnlijk dat ze het wisten maar dachten dat niemand het zou ontdekken, zegt Bos.

Een oplossing is niet zomaar voorhanden, zeggen de onderzoekers. De komende zeven jaar zit de wereld opgescheept met onveilige computers, omdat de ontwikkeling van nieuwe hardware veel tijd vergt en oude geheugens lang in gebruik blijven.

De onderzoekers hebben het rowhammerprobleem vier maanden geleden gemeld bij de fabrikanten. Die lijken het probleem niet serieus te nemen. Vanwege de grote veiligheidsrisico's brengen de onderzoekers hun vondst nu naar buiten. 's Werelds grootste geheugenfabrikant Samsung heeft niet gereageerd op vragen van *de Volkskrant*.

De onderzoekers hebben het probleem niet bij alle geheugenmodules ontdekt. Maar dat betekent niet dat deze veilig zijn. Mogelijk is een andere volgorde van 'hameren' nodig om een datalek te forceren. De onderzoekers komen een dezer dagen met een app waarmee gebruikers kunnen testen of hun smartphone gevoelig is voor het geheugenlek. Of er misbruik is gemaakt van de geheugenfout, is niet te zeggen. Bos: 'Reken maar dat geheime diensten hiermee bezig zijn.'