UPPSALA UNIVERSITET

2019-06-12 16:20 CEST

Ny metod täpper till beryktade säkerhetshål

Meltdown och Spectre är exempel på säkerhetshål i dagens mikroprocessorer som det hittills inte har funnits något effektivt försvar mot. De lösningar som finns adresserar endast specifika säkerhetshål utan att komma åt det underliggande problemet som orsakar säkerhetsbristerna. Nu kan forskare, från bland annat Uppsala universitet, presentera en bättre lösning.

Meltdown, Spectre och besläktade angrepp utnyttjar samma fundamentala säkerhetshål i mikroprocessorerna. De första angreppen uppdagades i fjol och de försvarsmöjligheter som har funnits har varit begränsade och även medfört att datorerna har blivit mycket långsammare.

Nu lägger forskare från Uppsala universitet, NTNU och Universidad de Murcia fram en bättre lösning som kommer att presenteras på International Symposium on Computer Architecture (ISCA) i slutet av juni. En konferens som samlar världens främsta forskare inom datorarkitektur. https://iscaconf.org/isca2019/

– Lösningen gör att prestandan, energieffektiviteten och säkerheten hos datorerna blir bättre jämfört med tidigare lösningar, säger Christos Sakalis, doktorand vid institutionen för informationsteknologi vid Uppsala universitet, som har varit med och utvecklat den nya metoden.

Säkerhetshålet uppstår när mikroprocessorn försöker att gissa sig till vad som ska göras härnäst. Sådan spekulation är det vanligaste tillvägagångssättet för att förbättra prestandan hos datamaskiner då det utnyttjar den fulla kapaciteten av mikroprocessorn.

– I teorin ska felaktiga gissningar inte efterlämna sig några spår, men gör det

likaväl, säger Alexandra Jimborean vid institutionen för informationsteknologi vid Uppsala universitet.

Dessa spår utnyttjar bland annat Meltdown och Spectre till att inhämta information från så kallade sidokanaler. Informationen används sedan för att kringgå säkerhetslösningar för att få tag på till exempel lösenord och krypteringsnycklar. Dessa sidokanaler har visat sig vara en akilleshäl inom datorsäkerhet. Arbetet med att hitta ett gott försvar har varit intensivt och världsomspännande, och nu har alltså en förbättrad lösning tagits fram.

– Vi har utvecklat en metod som gömmer alla spår av gissningarna, säger professor Stefanos Kaxiras, professor vid institutionen för informationsteknologi vid Uppsala universitet.

Metoden fördröjer delar av spekulationen och använder ett nytt sätt att förutspå talvärden, som är helt osynligt för utomstående.

Allt sker utan att försämra processorernas prestanda med mer än 11 procent och använder endast sju procent mer energi. Den tidigare lösningen försämrar prestandan med 46 procent och ökar energiförbrukningen med hela 51 procent.

– Vår metod kräver endast små ändringar av existerande processorer. Det, i kombination med den låga prestandaförsämringen, gör att metoden är enkel att realisera, säger Magnus Själander, gästforskare vid institutionen för informationsteknologi vid Uppsala universitet och førsteamenuensis på NTNU.

Christos Sakalis, Stefanos Kaxiras, Alberto Ros, Alexandra Jimborean, and Magnus Själander. 2019; Efficient Invisible Speculative Execution through Selective Delay and Value Prediction, presenteras vid The 46th Annual International Symposium on Computer Architecture (ISCA ’19), i slutet av juni. https://doi.org/10.1145/3307650.3322216

För mer information:

Stefanos Kaxiras, professor vid institutionen för informationsteknologi, Uppsala universitet,
epost: stefanos.kaxiras@it.uu.se, telefon: 018-471 29 74, mobiltelefon: 070-

425 03 94

Uppsala universitet - kvalitet, kunskap och kreativitet sedan 1477.Forskning i världsklass och högklassig utbildning till global nytta för samhälle, näringsliv och kultur. Uppsala universitet är ett av norra Europas högst rankade lärosäten. www.uu.se

Kontaktpersoner

Elin Bäckström
Presskontakt
Pressinformatör
Forskning, utbildning, övergripande
elin.backstrom@uadm.uu.se
018-471 17 06
070-425 09 83