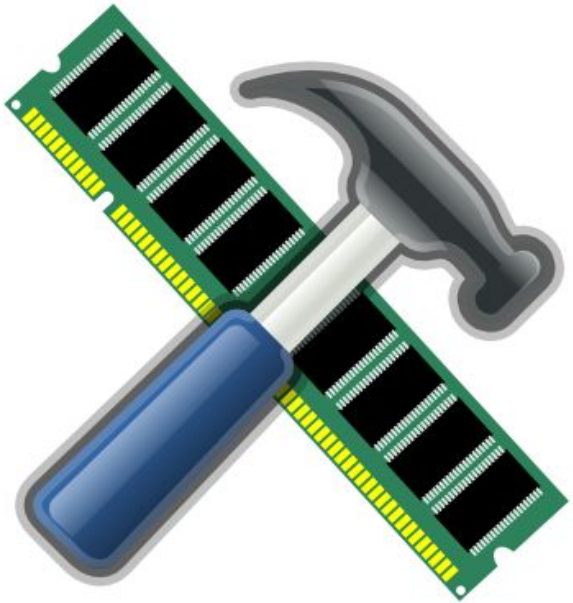
Row hammer

Dragan Simić

BarCamp Banjaluka 0x02
14. novembar 2015.

Sadržaj predavanja

- Šta je row hammer?
- Razlozi za njegovu pojavu
- Detaljnije o row hammer efektu
- Metode za njegovu prevenciju
- Uticaj na sigurnost
- Objavljeni sigurnosni eksploiti
- Diskusija, pitanja itd.



Šta je row hammer?

Neželjeni efekat prisutan u DRAM-u, izražen kroz curenje električnih naboja i moguću promjenu sadržaja (“bit flips”) memorijskih ćelija različitih od onih koje su zaista adresirane.

Otvara mogućnosti za potpuno zaobilaženje mehanizama zaštite memorije koji su prisutni unutar operativnih sistema, kroz direktnu manipulaciju hardverom.

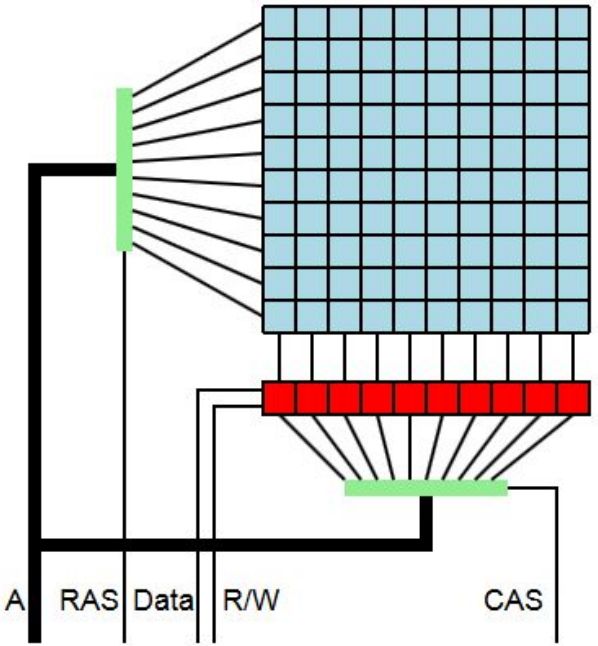
Prisustvo takvih efekata je poznato još od 1970-ih.

Razlozi za pojavu (I)

Svaka DRAM ćelija sačinjena je od po jednog kondenzatora i tranzistora, a naboj kondenzatora određuje “1” ili “0”.

Memorijske ćelije (plavi kvadrati na slici) su organizovane u matrice, a adresirane su kroz redove i kolone.

Memorijsku adresu obrađuju dekoderi reda i kolone (zeleni kvadrati).

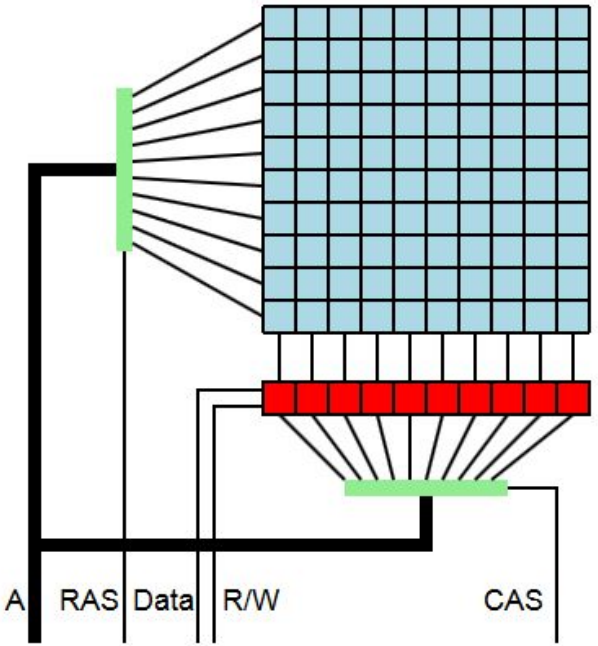


Razlozi za pojavu (II)

Adresa reda selektuje odn. aktivira red, i sadržaj svih bitova iz tog reda se pre-nosi u bafer reda (crveni kvadrati na slici).

Sadržaj čitavog reda mora da se nakon čitanja ponovo upiše nazad.

Usljed svoje prirode, DRAM zahtijeva periodično osvježavanje, a podložan je i nasumičnim promjenama sadržaja.



Row hammer efekat (I)

Velika gustina memorijskih ćelija u modernom DRAM-u uzrokuje povećan nivo interakcije između susjednih ćelija, koji rezultuje nasumičnim izmjenama sadržaja ćelija.

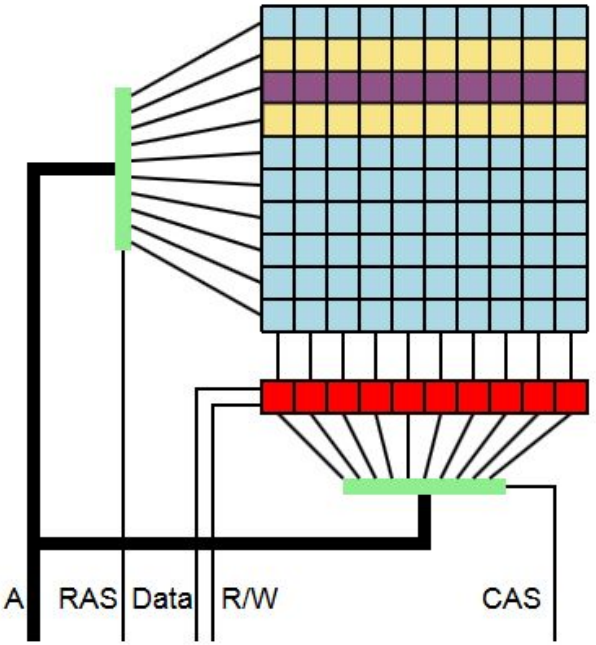
Proizvođači memorija su decenijama uspješno ugrađivali mehanizme za poništavanje “curenja”, ali je 2014. utvrđeno da je problem kod DDR3 DRAM-a ipak prisutan.

Utvrđeno je da su višestruke uzastopne aktivacije istih memorijskih redova unutar DDR3 DRAM-a osnovni uzrok.

Row hammer efekat (II)

Aktivacija reda memorijskih ćelija (ljubičasti kvadrati na slici) utiče na promjenu sadržaja susjednih redova (žuti kvadrati) ako njihov sadržaj nije osvježen prije nego što “curenje” pređe kritičnu granicu.

Promjena sadržaja je zabilježena nakon 139,000 uzastopnih pristupa, a jedna od 17,000 ćelija je bila podložna promjeni.



Metode prevencije (I)

Uobičajena *single-error correction and double-error detection* (SECDED) ECC memorija nije u mogućnosti da preduprijedi sve zabilježene promjene sadržaja.

Rasprostranjena ali manje efikasna i djelimično uspješna metoda prevencije je polovljenje intervala za osvježavanje DRAM-a (standardni interval je 64 ms).

Intel Xeon procesori, počevši od Ivy Bridge mikroarhitekture, podržavaju tzv. *pseudo target row refresh* (pTRR) DDR3 module.

Metode prevencije (II)

DDR4 memorija podržava tzv. *target row refresh* (TRR), koji uočava potencijalno ugrožene memorijske redove kroz brojanje pristupa redovima, i obavlja njihovo preventivno osvježavanje.

Row hammer eksploiti vrše veliki broj uzastopnih aktivacija memorijskih redova, čineći pri tome veliki broj nekeširanih pristupa memoriji koji se mogu brojiti i pratiti.

Pored specijalizovanih programa za provjeru “ranjivosti” hardvera, popularni memtest86 takođe sadrži row hammer test.

Uticaj na sigurnost

Zaštita memorije, kroz sprečavanje procesa da pristupe memoriji koja nije dodijeljena svakom od njih, predstavlja jedan od osnova rada većine modernih operativnih sistema.

Mijenjajući sadržaj memorijskih ćelija, row hammer zaobilazi sve nivoe softverskih metoda zaštite i omogućava proizvoljnu promjenu sadržaja memorije kroz direktnu manipulaciju hardverom.

Za poređenje, “konvencionalni” eksploiti rade na softverskom nivou i baziraju se na iskorištavanju programerskih grešaka.

Objavljeni sigurnosni eksploiti (I)

```
code1a:
  mov (X), %eax  // read from address X
  mov (Y), %ebx  // read from address Y
  clflush (X)    // flush cache for address X
  clflush (Y)    // flush cache for address Y
  jmp code1a
```

Ovaj segment asemblerskog koda za x86 arhitekturu demonstrira relativnu jednostavnost izazivanja row hammer efekta.

Memorijske adrese `X` i `Y` moraju biti izabrane tako da pripadaju različitim memorijskim redovima unutar iste memorijske banke.

Objavljeni sigurnosni eksploiti (II)

Prva istraživanja row hammer efekta, objavljena u 2014., nisu predviđala postojanje sigurnosnih problema.

U martu 2015., Project Zero je objavio dva sigurnosna eksploita koji koriste row hammer efekat za dobijanje dodatnih privilegija na x86-64 arhitekturi, oslanjajući se na `clflush` instrukciju.

Prvi objavljeni eksploit je usmjeren ka Googleovom Native Client (NaCl) mehanizmu za sandboxing, uspijevajući da na taj način izađe iz sandboxa i direktno izvrši sistemske pozive.

Objavljeni sigurnosni eksploiti (III)

Drugi Project Zero eksploit omogućava neprivilegovanom Linux procesu da dobije potpuni pristup RAM memoriji, kombinujući *heap spraying* i row hammer efekat da modifikuje *page table entries* (PTE) koji vrše povezivanje virtuelnih i fizičkih adresa.

U julu 2015., grupa istraživača je objavila jos jedan eksploit koji je nezavisan od arhitekture, i koji zaobilaženje CPU keševa ostvaruje specifičnim načinima pristupanja memoriji umjesto korištenjem `clflush` instrukcije. Objavljene su dvije varijante ovog eksploita, nativni kod i JavaScript implementacija.

Pitanja?

Za više detalja, spisak korištenih referenci itd.
https://en.wikipedia.org/wiki/Row_hammer

Autor ovog predavanja je ujedno primarni autor tog članka. :)