連載

5分で分かる!? 有名論文ナナメ読み

穐山空道（立命館大学）

Yoongu Kim et al. : Flipping Bits in Memory Without Accessing Them : An Experimental Study of DRAM Disturbance Errors

https://doi.org/10.1109/ISCA.2014.6853210

安全性にひそむ暗黙の仮定

皆さんは何かの安全性を考えたいとき，どのような議論をするだろうか？　まず起こり得るさまざまな状況を考え，それぞれに対して安全であることを議論するのが普通ではないかと思う．たとえば自宅のマンションに泥棒が入れないという安全性を考えよう．このとき起こり得る状況を（1）泥棒は玄関から侵入する，（2）泥棒は窓から侵入する，の2つであると思うと，（1）に対しては玄関がオートロックであること，（2）に対しては窓が電柱や雨水を通すパイプから離れていることから安全だと結論できるかもしれない．

実は上の議論には暗黙の仮定が潜んでおり，その仮定が成立しないと議論が無意味になってしまう．たとえば（2）に対する議論では，人間は電柱やパイプを伝わなければ高いところにはいけないはずだという仮定が潜んでいる．仮に最新のドローンの利用や超能力などによりこの仮定が崩れると，泥棒は窓から侵入することが可能になる．

ここで計算機の世界，特にソフトウェアの安全性を考える．たとえば異なるプロセスAとBがお互いのデータを読み書きできないという安全性がある．プロセスAは任意のアドレスにアクセスできるので，それでも絶対にプロセスBのデータにアクセスできないようにするために仮想アドレス空間が使用される．すなわち図-1のように異なるプロセスの仮想アドレスが物理アドレス空間上で重ならないようにすることで，プロセスAが全仮想アドレスにアクセスしようともプロセスBのデータには絶対に到達しないようになっている．

実は上の議論にも暗黙の仮定が潜んでいる．それは「あるデータはそれに対応する物理アドレスにアクセスしなければ読み書きできない」という仮定である．これはきわめてリーズナブルな仮定に思える．しかし本論文はこの仮定が成り立たないことを実際に市販されている機器を使って証明してしまったのである．

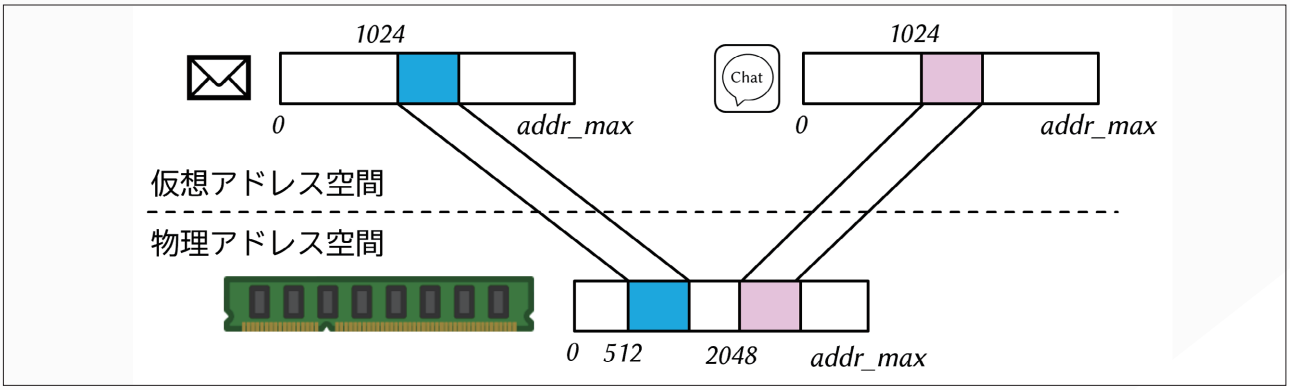

図-1　異なるプロセスの仮想アドレス空間は物理アドレス空間上では分離されている

メモリの仕組み

本論文の対象である DRAM (Dynamic Random Access Memory) の仕組みをまず概説する．DRAM は現代のほとんどすべての計算機のメインメモリに利用されるデバイスである．PC だけでなくスーパーコンピュータ，スマートフォン，ゲーム機などさまざまな形態の計算機が DRAM を利用している．

DRAM 上のデータは行列上に並んだ微小なキャパシタの電荷の有無で表現され，キャパシタ 1 つが 1 ビットを表現する．データを読み書きするにはまず行列の一行分のすべてのキャパシタの電荷を sense amplifier と呼ばれる回路で検知し，その後 sense amplifier に蓄えられたデータを CPU に転送したり CPU からのデータで上書きしたりする．このように一行分の電荷をすべて検知する操作を activation と呼ぶ．

DRAM のもう 1 つ重要な操作に refresh がある．DRAM を構成するキャパシタは微小ですぐに電荷が抜けてしまうため定期的な電荷の貯め直しが必要であり，この貯め直し操作を refresh と呼ぶ．近年の DRAM では各行は少なくとも 64 ms に一度 refresh しなければならないと定められている．

RowHammer 攻撃

本論文は RowHammer と呼ばれる攻撃により「あるキャパシタを含む行に直接アクセスせずともそのキャパシタの表すデータが書換可能である」ことを，市販の DRAM で実際に示した．なお類似の特許が本論文以前に出願されていたが，本論文はこれらの特許の一般公開より前に投稿されたとのことである．これを以て，研究業界では一般に本論文が RowHammer 攻撃の発見者とされている．

RowHammer 攻撃の手順はシンプルである．いま攻撃対象となるデータを保持するキャパシタを含む行を行 V（Victim），その隣の行を行 A（Aggressor）とする．このとき攻撃者が行 A を何度も activation すると，電磁気的な影響により行 V に含まれるキャパシタの電荷が通常よりも速く抜ける．攻撃者は行 V が refresh される 64 ms の間にこれを繰り返すことで攻撃対象のデータを書き換えることができる．

ソフトウェア的な視点でもう一度攻撃の原理を見てみよう．いま攻撃者のプロセス A と，被攻撃者のプロセス B がある．プロセス A と B は前述のとおり異なる仮想アドレス空間を使用するため，プロセス A が取り得るすべての仮想アドレスにアクセスしてもプロセス B のデータには直接アクセスはできない．しかし DRAM 上では，プロセス A の仮想アドレス $\mathrm{Addr_A}$ に対応する行とプロセス B の仮想アドレス $\mathrm{Addr_B}$ に対応する行が隣り合う可能性がある．このとき攻撃者は仮想アドレス $\mathrm{Addr_A}$ に何度もアクセスすることで被攻撃者のデータを書換できてしまう．

市販の DRAM での実験

本論文の大きな貢献は，RowHammer 攻撃が市販の DRAM で実際に成功することを示し，その特性を詳細に分析したことである．具体的には，大手メーカ 3 社の製造する DRAM チップを搭載したメモリモジュールを合計 129 本複数購入し，それらのメモリに FPGA を用いて activation などの操作を適用する実験を行った．なお 3 社と聞くと少ないと思うかもしれないが，「メモリモジュール」のメーカは数多あるもののそこ搭載する「DRAM チップ」のメーカは世界でも Micron, Samsung, SKHynix, ISSI など少数しかない．

本論文で発見された興味深い特性を 2 点紹介する．1 点目は「製造年が古い DRAM チップでは攻撃はほとんど成功しない」という特性である．3 メーカすべての DRAM で，2010/2011 年頃以前に製造されたチップでは攻撃が成功しなかった．本論文ではこれを製造プロセスの更新（微細化）によるものと推測している．すなわち DRAM の容量増加を実現するための微細化により行同士の距離が近くなることで，より攻撃が成功しやすくなる（逆に過去のチップでは攻撃が成功しない）と考えられている．

もう1点の興味深い特性は，「攻撃が成功するキャパシタと弱いキャパシタは一致しない」ということである．ここで「弱い」とは，攻撃を受けていない通常状態において電荷の抜ける速度が速いこととする．すべてのキャパシタは最低でも 64 ms の間データを保持することが要求されるが，実際には「強い」キャパシタはその何倍も時間データを保持できることが知られている．本論文では refresh や activation 操作を 10 秒間行わない実験をしてデータが破壊されたキャパシタを「弱い」と定義した．それらを RowHammer 攻撃によって値を書換可能だったキャパシタと比較したところ，ほとんど相関が見られなかったと報告している．

さらに攻撃を発展させる研究

本論文で発見された RowHammer 攻撃はある意味基礎的なものであった．しかしその後数多くの研究が行われさまざまな発展攻撃が発見されている．有名なものの1つが RAMBleed[1] で，これは RowHammer 攻撃におけるデータの壊れ方が隣の行のデータに依存することを利用し，自らのデータを破壊することでその隣の行のデータを推測する攻撃である．すなわち RowHammer 攻撃を応用しデータの「読み込み」を実現したのである．

参考文献

1) Kwong, A. et al. : RAMBleed : Reading Bits in Memory Without Accessing Them, IEEE S&P'20.

(2023 年 4 月 24 日受付)

穐山空道（正会員）
s-akym@fc.ritsumei.ac.jp
2015 年東京大学大学院情報理工学系研究科創造情報学専攻修了．博士（情報理工学）．NTT，産業技術総合研究所，東京大学助教を経て，2022 年より立命館大学情報理工学部セキュリティ・ネットワークコース准教授．