COLD BOOT ATTACK

on DDR2 and DDR3 RAM

Simon Lindenlauf, Marko Schuba, Hans Höfken
Aachen University of Applied Sciences, Germany
About

• Simon Lindenlauf
  • former BSc, now Master student at Aachen University of Applied Sciences (FH Aachen)
  • cold boot: topic of his bachelor thesis

• Marko Schuba
  • professor at FH Aachen (computer science)
  • topics of interest: security, forensics

• Hans Höfken
  • researcher at FH Aachen
  • topics of interest: practical stuff, ethical hacking etc.
Agenda

- What is a cold boot attack?
- Previous work by others
- Experiments
- Results
- Conclusions
DRAM

- DRAM = Dynamic Random-Access Memory
  - is a type of RAM
  - each bit stored in separate capacitor within integrated circuit (states: charged / discharged)
- Leakage and refresh
  - capacitors leak, i.e. they slowly discharge
  - periodic refresh necessary (memory is “dynamic”)
- DRAM is main memory in computers today
  - high density, compared to static RAM
DDR SDRAM*

- DDR SDRAM is a widely used DRAM type
  - Types: DDR1, DDR2, DDR3 and recently DDR4
  - Have different peak transfer rates
    - basically doubling it with each generation
  - Most computers today use DDR2 or DDR3 SDRAM

* Double data rate synchronous dynamic random-access memory
Refresh Rates & Retention Times

• As mentioned before: memory cells leak and thus require refresh

• Refresh rate depends on temperature
  • up to 85°C (185°F): 64 ms (standard refresh time)
  • between 85°C (185°F) and 95°C (203°F): 32 ms
  • obviously: leakage of cells increases with temperature

• 64 ms refresh threshold to be on the safe side...
  • e.g. tests with DDR3
  • 45°C (113°F)
  • retention time for all cells >= 1.5 s

cooling RAM increases retention time
What is cold boot?

- Two options for rebooting a machine
  - cold reboot (or cold boot, hard boot)
  - warm reboot (or soft reboot)

- **Warm reboot** (simplified)
  - restarting machine while it is powered on
    - e.g. Ctrl-Alt-Del on Windows, kexec on Linux

- **Cold boot** (simplified)
  - restarting machine from a power-less state
    - disconnecting cord/battery and starting machine again
What is a cold boot attack?

**Basic idea**

- DRAM memory content can be extracted after power has been cut
- the lower the temperature of the DRAM the higher the probability that memory is unchanged

**Two ways to do it...memory dump can be done**

- on the original machine
  - DRAM stays where it is
  - original machine is cold booted
- or on a different machine
  - DRAM is removed and plugged into a different computer
  - different computer is cold booted
Why all this?

- **Main purpose:** recovery of hard disk encryption key
- **Case:** You are a digital forensics investigator
  - running machine which uses hard disk encryption
- **Machine not screen-locked:** simple
- **Machine is screen-locked** (& password unknown)
  - cannot simply copy disk
  - cannot shut down machine (& take out hard disk)
  - decryption key is in RAM: but as machine is locked, no way to dump image from the machine directly
- **Cold boot attack can help**
  - attack provides an image of the RAM
  - might contain errors… but still keys can be recovered

Agenda

• What is a cold boot attack?
• Previous work by others
• Experiments
• Results
• Conclusions
Lest We Remember...

- Halderman et al. published work on Cold Boot Attacks on Encryption Keys at USENIX Security '08
- DDR and DDR2 SDRAM
On the Practicability of Cold Boot...

- 2013 Gruhn and Müller provide results for different DDR types 1, 2 and 3
  - Result: „we could not reproduce cold boot attacks against modern DDR3 chips“
So, no cold boot attack on DDR3?

- Let’s try it out...
  - What could be done differently?
  - Obvious...
    different picture...

Mona ⇒ Lena
So, no cold boot attack on DDR3?

- Let's try it out...
  - What could be done differently?
  - Obvious... different picture...
    Mona ⇒ Lena
  - Ok, maybe something else...
    Mainboard
  - But first a step back...

http://www.aliexpress.com/item-/For-ASUS-60-N0GMB1800-B02-Laptop-motherboard-mainboard-K53SV-REV-3-0-45-days-warranty-works/1866829087.html
Agenda

- What is a cold boot attack?
- Previous work by others
- Experiments
- Results
- Conclusions
Considerations

- Cold boot attack results depend on
  - DRAM types ⇒ DDR2 and DDR3
  - DRAM manufacturer ⇒ 7 different manufacturers
  - individual DRAM ⇒ 16 different ones tested
## Module Overview

<table>
<thead>
<tr>
<th>Type</th>
<th>Manufact.</th>
<th>Module Name</th>
<th>Capacity</th>
<th>Freq. / MHz</th>
<th>Production Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>Hynix</td>
<td>HYMP564U64CP8-Y5</td>
<td>512 MB</td>
<td>333.33 MHz</td>
<td>2006 Woche 49</td>
</tr>
<tr>
<td>B</td>
<td>Samsung</td>
<td>M3 78T6553EZS-CE6</td>
<td>512 MB</td>
<td>333.33 MHz</td>
<td>2007 Woche 13</td>
</tr>
<tr>
<td>C</td>
<td>Kingston</td>
<td>E5108AGBG</td>
<td>1024 MB</td>
<td>333.33 MHz</td>
<td>2007 Woche 13</td>
</tr>
<tr>
<td>D</td>
<td>Kingston</td>
<td>E5108AGBG</td>
<td>1024 MB</td>
<td>333.33 MHz</td>
<td>2007 Woche 13</td>
</tr>
<tr>
<td>E</td>
<td>Hexon</td>
<td>HY5PS12821C</td>
<td>1024 MB</td>
<td>400 MHz</td>
<td>2008 Woche 19</td>
</tr>
<tr>
<td>F</td>
<td>G Skill</td>
<td>F2-8000CL5-2GBPQ</td>
<td>2048 MB</td>
<td>400 MHz</td>
<td>2008 (Kaufdatum)</td>
</tr>
<tr>
<td>G</td>
<td>Kingston</td>
<td>2G-UDIMM</td>
<td>2048 MB</td>
<td>400 MHz</td>
<td>2009 Woche 3</td>
</tr>
<tr>
<td>H</td>
<td>Kingston</td>
<td>2G-UDIMM</td>
<td>2048 MB</td>
<td>400 MHz</td>
<td>2011 Woche 30</td>
</tr>
<tr>
<td>I</td>
<td>Transcend</td>
<td>JM367Q643A-6</td>
<td>512 MB</td>
<td>333.33 MHz</td>
<td>-</td>
</tr>
<tr>
<td>J</td>
<td>Kingston</td>
<td>S330110</td>
<td>1024 MB</td>
<td>400 MHz</td>
<td>-</td>
</tr>
<tr>
<td>K</td>
<td>Transcend</td>
<td>JM800QU-1G</td>
<td>1024 MB</td>
<td>400 MHz</td>
<td>-</td>
</tr>
<tr>
<td>L</td>
<td>Hynix</td>
<td>HMT325S6BFR8C-H9</td>
<td>2048 MB</td>
<td>666.67 MHz</td>
<td>2011 Woche 43</td>
</tr>
<tr>
<td>M</td>
<td>Hynix</td>
<td>HMT112S6AFR6C-G7</td>
<td>1024 MB</td>
<td>533.33 MHz</td>
<td>2011 (Kaufdatum)</td>
</tr>
<tr>
<td>N</td>
<td>Corsair</td>
<td>CM3X2GSD1066</td>
<td>2048 MB</td>
<td>533.33 MHz</td>
<td>2011 (Kaufdatum)</td>
</tr>
<tr>
<td>O</td>
<td>Kingston</td>
<td>KVR16N11S8/4</td>
<td>4096 MB</td>
<td>800 MHz</td>
<td>2013 Woche 24</td>
</tr>
<tr>
<td>P</td>
<td>Samsung</td>
<td>M378B5173DB0-CK0</td>
<td>4096 MB</td>
<td>800 MHz</td>
<td>2013 Woche 48</td>
</tr>
</tbody>
</table>
Considerations

- Cold boot attack results depend on
  - DRAM types \( \Rightarrow \) DDR2 and DDR3
  - DRAM manufacturer \( \Rightarrow \) 7 different manufacturers
  - individual DRAM \( \Rightarrow \) 16 different ones tested
  - mainboard \( \Rightarrow \) 2 different ones
Mainboards used

GA-G41M-Combo

Notebook ASUS P53E mainboard
Considerations

- **Cold boot attack results depend on**
  - DRAM types ⇒ DDR2 and DDR3
  - DRAM manufacturer ⇒ 7 different manufacturers
  - individual DRAM ⇒ 16 different ones tested
  - mainboard ⇒ 2 different ones
  - Multi Channel Mode? ⇒ if yes, several impacts
  - DRAM temperature ⇒ tested different ones
  - DRAM seconds w/o power ⇒ tested different ones
  - footprint of cold boot OS ⇒ the smaller the better
Procedure

- **Steps of cold boot attack**
  - original machine: prepare it with test data \( \text{(Lena + x)} \)
  - cold boot machine: prepare boot USB stick & connect it
  - original machine (running): adjust DRAM temperature (e.g. cool it to increase retention time)
  - original machine: power it down
    - unplug power cable
      (notebook: battery to be removed before)
  - if original ≠ cold boot machine then move DRAM
  - cold boot machine: power-on (booting from USB)
  - program on USB stick reads and stores RAM data
  - analyse RAM data (offline)
Procedure

- **Cold boot attack procedure**
  - prepare boot USB stick & connect it to cold boot machine
  - prepare original machine with test data (Lena)
  - cool DRAM on running original machine (to increase retention time)
  - power down original machine
  - remove battery
  - unplug power cable
  - if original ≠ cold boot machine:
    - move DRAM
  - power on cold boot machine (booting from USB)
  - program on USB stick reads and stores RAM data
  - analyse RAM data (offline)

**Cold boot attack**

1. prepare data & USB
2. cool DRAM
3. power down
4. (move DRAM)
5. power-on & read data
Prepare Test Data

- **Task:** same data in memory for each test
  - used small OS based on JamesM’s kernel development tutorials (multiboot kernel) and GRUB bootloader
  - test data based on Lena image (X PixMap)
  - pixel area extracted and written to RAM (starting at fixed address)
  - additionally: 100 MB test file (starting at another fixed address)
Prepare Cold Boot USB

- Two small footprint OS (~ 2 MB) tested
  - msramdmp (Wesley McGrew; 32 bit OS)
    - used predominantly (single USB stick / multiple tests)
  - bios_memimage (Princeton University, 64 bit OS)
    - for DRAM > 4 GB
- When machine is cold booted from USB
  - both dump the RAM and save it to USB stick
  - msramdmp slightly modified to extract test data only
    - first 500 MB of DRAM
    - faster and sufficient for test data
How to cool the DRAM?

• Option 1: move project to a cold location...
• Option 2: more cost efficient
  ⇒ cooling spray
Check Temperature

Cool DRAM

Measure Time

Cold boot attack
1. prepare data & USB
2. cool DRAM
3. power down
4. (move DRAM)
5. power-on & read data
Read & Analyse Data

• Determine byte & bit errors
Read & Analyse Data

- Determine byte & bit errors
- Reconstruct & view image

a) bit errors that change byte to quote character or null byte damage whole line

b) correction of quote characters and null bytes by one bit reduce this to pixel errors
Video not included in pdf
Agenda

• What is a cold boot attack?
• Previous work by others
• Experiments
• Results
• Conclusions
# Module Overview

<table>
<thead>
<tr>
<th>Type</th>
<th>Manufact.</th>
<th>Module Name</th>
<th>Capacity</th>
<th>Freq. / MHz</th>
<th>Production Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>Hynix</td>
<td>HYMP564U64CP8-Y5</td>
<td>512 MB</td>
<td>333.33</td>
<td>2006 Woche 49</td>
</tr>
<tr>
<td>B</td>
<td>Samsung</td>
<td>M3 78T6553E2S-CE6</td>
<td>512 MB</td>
<td>333.33</td>
<td>2007 Woche 13</td>
</tr>
<tr>
<td>C</td>
<td>Kingston</td>
<td>E5108AGBG</td>
<td>1024 MB</td>
<td>333.33</td>
<td>2007 Woche 13</td>
</tr>
<tr>
<td>D</td>
<td>Kingston</td>
<td>E5108AGBG</td>
<td>1024 MB</td>
<td>333.33</td>
<td>2007 Woche 13</td>
</tr>
<tr>
<td>E</td>
<td>Hexon</td>
<td>HY5PS12821C</td>
<td>1024 MB</td>
<td>400</td>
<td>2008 Woche 19</td>
</tr>
<tr>
<td>F</td>
<td>G Skill</td>
<td>F2-8000CL5-2GBPQ</td>
<td>2048 MB</td>
<td>400</td>
<td>2008 (Kaufdatum)</td>
</tr>
<tr>
<td>G</td>
<td>Kingston</td>
<td>2G-UDIMM</td>
<td>2048 MB</td>
<td>400</td>
<td>2009 Woche 3</td>
</tr>
<tr>
<td>H</td>
<td>Kingston</td>
<td>2G-UDIMM</td>
<td>2048 MB</td>
<td>400</td>
<td>2011 Woche 30</td>
</tr>
<tr>
<td>I</td>
<td>Transcend</td>
<td>JM367Q643A-6</td>
<td>512 MB</td>
<td>333.33</td>
<td></td>
</tr>
<tr>
<td>J</td>
<td>Kingston</td>
<td>S330110</td>
<td>1024 MB</td>
<td>400</td>
<td></td>
</tr>
<tr>
<td>K</td>
<td>Transcend</td>
<td>JM800QJU-1G</td>
<td>1024 MB</td>
<td>400</td>
<td></td>
</tr>
<tr>
<td>L</td>
<td>Hynix</td>
<td>HMT325S6BFR8C-H9</td>
<td>2048 MB</td>
<td>666.67</td>
<td>2011 Woche 43</td>
</tr>
<tr>
<td>M</td>
<td>Hynix</td>
<td>HMT112S6AFR6C-G7</td>
<td>1024 MB</td>
<td>533.33</td>
<td>2011 (Kaufdatum)</td>
</tr>
<tr>
<td>N</td>
<td>Corsair</td>
<td>CM3X2GSD1066</td>
<td>2048 MB</td>
<td>533.33</td>
<td>2011 (Kaufdatum)</td>
</tr>
<tr>
<td>O</td>
<td>Kingston</td>
<td>KVR16N11S8/4</td>
<td>4096 MB</td>
<td>800</td>
<td>2013 Woche 24</td>
</tr>
<tr>
<td>P</td>
<td>Samsung</td>
<td>M378B5173DB0-CK0</td>
<td>4096 MB</td>
<td>800</td>
<td>2013 Woche 48</td>
</tr>
</tbody>
</table>
Selected Results DDR2

10s without power at -35°C to -30°C

<table>
<thead>
<tr>
<th>DDR2</th>
<th>RAM</th>
<th>Byte Errors</th>
<th>Bit Errors</th>
<th>Byte Error Rate</th>
<th>Bit Error Rate</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>B</td>
<td>236</td>
<td>236</td>
<td>0.000236%</td>
<td>0.000030%</td>
</tr>
<tr>
<td>2</td>
<td>F</td>
<td>2.204</td>
<td>2.212</td>
<td>0.002204%</td>
<td>0.000277%</td>
</tr>
<tr>
<td>3</td>
<td>G</td>
<td>3.675</td>
<td>3.943</td>
<td>0.003675%</td>
<td>0.000493%</td>
</tr>
<tr>
<td>4</td>
<td>C</td>
<td>82.539</td>
<td>85.766</td>
<td>0.0825%</td>
<td>0.0107%</td>
</tr>
<tr>
<td>5</td>
<td>H</td>
<td>239.263</td>
<td>558.522</td>
<td>0.239%</td>
<td>0.070%</td>
</tr>
<tr>
<td>6</td>
<td>D</td>
<td>729.380</td>
<td>795.702</td>
<td>0.729%</td>
<td>0.099%</td>
</tr>
<tr>
<td>7</td>
<td>J</td>
<td>2.248.293</td>
<td>2.477.976</td>
<td>2.248%</td>
<td>0.310%</td>
</tr>
<tr>
<td>8</td>
<td>I</td>
<td>4.763.617</td>
<td>7.862.582</td>
<td>4.764%</td>
<td>0.983%</td>
</tr>
<tr>
<td>9</td>
<td>A</td>
<td>12.870.663</td>
<td>28.379.907</td>
<td>12.87%</td>
<td>3.55%</td>
</tr>
<tr>
<td>10</td>
<td>E</td>
<td>20.997.916</td>
<td>71.909.648</td>
<td>21.00%</td>
<td>8.99%</td>
</tr>
<tr>
<td>11</td>
<td>K</td>
<td>35.475.736</td>
<td>88.992.338</td>
<td>35.48%</td>
<td>11.12%</td>
</tr>
</tbody>
</table>
Selected Results DDR3

10s without power at -35°C to -30°C

<table>
<thead>
<tr>
<th>DDR3</th>
<th>RAM</th>
<th>Byte Errors</th>
<th>Bit Errors</th>
<th>Byte Error Rate</th>
<th>Bit Error Rate</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>N</td>
<td>1.604</td>
<td>5.624</td>
<td>0.001604%</td>
<td>0.000703%</td>
</tr>
<tr>
<td>2</td>
<td>M</td>
<td>4.435</td>
<td>8.275</td>
<td>0.004435%</td>
<td>0.001034%</td>
</tr>
<tr>
<td>3</td>
<td>L</td>
<td>460.860</td>
<td>534.566</td>
<td>0.461%</td>
<td>0.067%</td>
</tr>
</tbody>
</table>
Error – Temperature Dependency

Temperature Dependency

Byte Errors (for 100 MB test data)

Temperature in °C (measured 15s after power-off)

exponential trend line
(a) -35°C and 0.041% Byte Error Rate
(b) -5°C and 0.273% Byte Error Rate
(c) +15°C and 1.756% Byte Error Rate
(d) +30°C and 34.284% Byte Error Rate
Error - Time Dependency

-Time Dependency

Byte Errors (for 100 MB test data)

Time without power in s

- exponential trend line
- temperature -20°C
Error Patterns

• some DRAM show different error rates depending on ground state
• some areas error free
• reason not clear yet

Bereich 1: Muster FFFF FFFF FFFF FFFF
Bereich 2: Muster FFFF FFFF 0000 0000
Bereich 3: Muster 0000 0000 0000 0000
Bereich 2: Muster FFFF FFFF 0000 0000
Bereich 3: Muster 0000 0000 0000 0000
Bereich 2: Muster FFFF FFFF 0000 0000
Anti Cold Boot

- Enable POST in BIOS
  - overwrite complete RAM
- Password-protect boot device sequence
  - avoid booting of RAM dump software
- Password based pre-boot authentication
  - otherwise encryption key in RAM after restart
- Store encryption key outside RAM
  - e.g. possible in CPU registers
  - this even works if RAM is moved to different machine
Agenda

• What is a cold boot attack?
• Previous work by others
• Experiments
• Results
• Conclusions
Conclusions

• Cold boot attacks not as complicated as expected😊
  • could be feasible approach for digital forensics investigators

• Attacks on DDR3 are possible
  • admittedly, we have been lucky with the board…
Thank You

Marko Schuba
Aachen University of Applied Sciences
Germany
schuba@fh-aachen.de