As if Time Had Stopped – Checking Memory Dumps for Quasi-Instantaneous Consistency

Jenny Ottmann, Üsame Cengiz, Frank Breitinger, Felix Freiling

Chair of IT Security Infrastructures
Friedrich-Alexander-Universität Erlangen-Nürnberg
Inconsistencies in Memory Dumps

- Inhibit the analysis
- Not that easy to measure

1. Case and Richard III 2017; Pagani, Fedorov, and Balzarotti 2019
2. Vömel and Stüttgen 2013; Gruhn and Freiling 2016
Inconsistencies in Memory Dumps

- Inhibit the analysis
- Not that easy to measure

1. Case and Richard III 2017; Pagani, Fedorov, and Balzarotti 2019
2. Vömel and Stüttgen 2013; Gruhn and Freiling 2016
Inconsistencies in Memory Dumps

- Inhibit the analysis
- Not that easy to measure

---

1. Case and Richard III 2017; Pagani, Fedorov, and Balzarotti 2019
2. Vömel and Stüttgen 2013; Gruhn and Freiling 2016
Inconsistencies in Memory Dumps

• Inhibit the analysis
• Not that easy to measure

1 Case and Richard III 2017; Pagani, Fedorov, and Balzarotti 2019
2 Vömel and Stüttgen 2013; Gruhn and Freiling 2016
Inconsistencies in Memory Dumps

1 Case and Richard III 2017; Pagani, Fedorov, and Balzarotti 2019
2 Vömel and Stütten 2013; Gruhn and Freiling 2016
Inconsistencies in Memory Dumps

- Inhibit the analysis\(^1\)

---

\(^1\)Case and Richard III 2017; Pagani, Fedorov, and Balzarotti 2019
\(^2\)Vömel and Stütten 2013; Gruhn and Freiling 2016
Inconsistencies in Memory Dumps

- Inhibit the analysis\(^1\)
- Not that easy to measure\(^2\)

---

\(^1\) Case and Richard III 2017; Pagani, Fedorov, and Balzarotti 2019
\(^2\) Vömel and Stütten 2013; Gruhn and Freiling 2016
Consistency Indicators

Memory dump

Level of consistency

3Pagani, Fedorov, and Balzarotti 2019
Consistency Indicators

- Already existent
  E.g., VMA count, process list

---

\(^3\)Pagani, Fedorov, and Balzarotti 2019
Consistency Indicators

- Already existent
  E.g., VMA count \(^3\), process list
- Deliberately placed

\(^3\)Pagani, Fedorov, and Balzarotti 2019
Consistency Indicators

- Already existent
  E.g., VMA count \(^3\), process list
- Deliberately placed
  → Observe quasi-instantaneous consistency

\(^3\)Pagani, Fedorov, and Balzarotti 2019
Model
Set of $n$ memory regions: $R = \{r_1, \ldots, r_n\}$

Memory: $m: R \times T \rightarrow V$

Only events change contents, therefore, $T$ is defined as the set of natural numbers $\mathbb{N}$

Snapshot: $s: R \rightarrow V \times T$
• Set of $n$ memory regions:
  \[ R = \{ r_1, \ldots, r_n \} \]
Space-Time Diagrams

- Set of $n$ memory regions:
  \[ R = \{ r_1, \ldots, r_n \} \]

- Memory: $m : R \times T \rightarrow V$
Set of $n$ memory regions:
\[ R = \{ r_1, \ldots, r_n \} \]

Memory: \( m : R \times T \rightarrow V \)

Only events change contents,
Set of $n$ memory regions:

$$R = \{ r_1, \ldots, r_n \}$$

Memory: $m : R \times T \rightarrow V$

Only events change contents, therefore, $T$ is defined as the set of natural numbers $\mathbb{N}$.
Set of $n$ memory regions:
\[ R = \{ r_1, \ldots, r_n \} \]

Memory: \[ m : R \times T \to V \]

Only events change contents, therefore, $T$ is defined as the set of natural numbers $\mathbb{N}$

Snapshot: \[ s : R \to V \times T \]
Quasi-Instantaneous Consistency
Ideal Case of Memory Acquisition

Instantaneous Consistency$^4$

$^4$Ottmann, Breitinger, and Freiling 2022.
Ideal Case of Memory Acquisition

Instantaneous Consistency\(^4\)

\[^4\text{Ottmann, Breitinger, and Freiling 2022.}\]

Ottmann et al. FAU Erlangen-Nürnberg
Quasi-Instantaneous Consistency\textsuperscript{5}

\textsuperscript{5}Ottmann, Breitinger, and Freiling 2022.
Approximation

Quasi-Instantaneous Consistency\textsuperscript{5}

\textsuperscript{5}Ottmann, Breitinger, and Freiling 2022.
Observing Quasi-Instantaneous Consistency
Idea

Known states
- 13:05
13:01 13:01
- -

\[ t: 1 \quad 2 \]
Idea

Known states

\[ r_1 \quad 13:01 \quad r_2 \quad 13:01 \quad r_3 \quad 13:01 \quad s_1 \quad 13:05 \]

<table>
<thead>
<tr>
<th>t</th>
<th>1</th>
<th>2</th>
</tr>
</thead>
<tbody>
<tr>
<td>13:01</td>
<td>13:01</td>
<td></td>
</tr>
<tr>
<td>13:05</td>
<td>-</td>
<td></td>
</tr>
<tr>
<td>-</td>
<td>-</td>
<td></td>
</tr>
</tbody>
</table>

Ottmann et al. FAU Erlangen-Nürnberg
Idea

Known states

<table>
<thead>
<tr>
<th>t</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
</tr>
</thead>
<tbody>
<tr>
<td>13:01</td>
<td>13:01</td>
<td>13:01</td>
<td>13:08</td>
<td>13:08</td>
<td>-</td>
</tr>
<tr>
<td>-</td>
<td>13:06</td>
<td>13:06</td>
<td>13:06</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>-</td>
<td>13:05</td>
<td>13:05</td>
<td>13:05</td>
<td>13:09</td>
<td>-</td>
</tr>
</tbody>
</table>

Ottmann et al. FAU Erlangen-Nürnberg
Local counters & global counter array
Local counters & global counter array

- Detection of events
- Ability to save counters locally
- Ability to save counters in global counter array
Observation Elements

Local counters & global counter array

Prerequisites

- Detection of events

Ottmann et al. FAU Erlangen-Nürnberg
Observation Elements

Local counters & global counter array

Prerequisites

- Detection of events
- Ability to save counters locally
- Ability to save counters in global counter array
Formal Proof
We want to show that:

- Local counters & global counter array suffice to check quasi-instantaneous consistency
Only events change contents
Normalized Snapshot $N(s)$

Only events change contents

$r_1\quad N(s)\quad r_2\quad s\quad r_3$

$r_1: t = r_2: t = r_3: t = 3$

$r_1: t = 2\quad r_2: t = 1\quad r_3: t = 3$
Normalized Snapshot $N(s)$

**Only events change contents**

Times

- $s$: $r_1.t = r_2.t = r_3.t = 3$
**Only events change contents**

- \( r_1 \cdot t = r_2 \cdot t = r_3 \cdot t = 3 \)

**Times**

- \( s \)
  - \( r_1 \cdot t = 2 \)
  - \( r_2 \cdot t = 1 \)
  - \( r_3 \cdot t = 3 \)
A snapshot is quasi-instantaneous if a hypothetical \textit{instantaneous} snapshot with the same values exists.
A snapshot is quasi-instantaneous if a hypothetical *instantaneous* snapshot with the same values exists.
We can use $\hat{s}$ to determine if the snapshot is quasi-instantaneous.
We can use \( \hat{s} \) to determine if the snapshot is quasi-instantaneous.

\[
N(\hat{s}) = N(s)
\]
Example

\[
\begin{array}{c}
\begin{array}{c}
G \\
0 & 2 & 2 & 2 & 5 \\
1 & 1 & 1 & 4 & 4 \\
0 & 0 & 3 & 3 & 3 \\
\end{array}
\end{array}
\]

Ottmann et al. FAU Erlangen-Nürnberg
Example

\[ G \]

\[
\begin{array}{cccccc}
0 & 2 & 2 & 2 & 5 \\
1 & 1 & 1 & 4 & 4 \\
0 & 0 & 3 & 3 & 3 \\
\end{array}
\]

**t:** 0 1 2 3 4 5

Ottmann et al. FAU Erlangen-Nürnberg
Example

$T_{N(s_1)} = (2, 1, 0)$
Example

\[ T_{N(s_1)} = (2, 1, 0) \]
\[ T_{N(\hat{s}_1)} = (2, 1, 0) \]
Example

\[ T_N(s_1) = (2, 1, 0) \]

\[ T_N(\hat{s}_1) = (2, 1, 0) \]
Example

\[ T_N(s_1) = (2, 1, 0) \]

\[ T_N(\hat{s}_1) = (2, 1, 0) \]

\[ T_N(s_2) = (5, 1, 3) \]
Example

\( s_1 \)
- \( T_{N(s_1)} = (2, 1, 0) \)
- \( T_{N(\hat{s}_1)} = (2, 1, 0) \)

\( s_2 \)
- \( T_{N(s_2)} = (5, 1, 3) \)
- \( T_{N(\hat{s}_2)} = (5, 4, 3) \)

---

Ottmann et al. FAU Erlangen-Nürnberg
Practical Evaluation
Pivot Program

 Threads

 Global counter array

 $r_1$  

 local counter

 $r_n$

 local counter

 Ottmann et al. FAU Erlangen-Nürnberg
Global Counter Array Simplification

\begin{center}
\begin{tikzpicture}
\node (r1) at (0,0) [circle,fill,inner sep=2pt] {$r_1$};
\node (e1) at (2,0) [circle,fill,inner sep=2pt] {$e_1$};
\node (r2) at (0,-2) [circle,fill,inner sep=2pt] {$r_2$};
\node (e2) at (2,-2) [circle,fill,inner sep=2pt] {$e_2$};
\node (e3) at (2.5,-2) [circle,fill,inner sep=2pt] {$e_3$};
\node (e5) at (3,-2) [circle,fill,inner sep=2pt] {$e_5$};
\node (r3) at (0,-4) [circle,fill,inner sep=2pt] {$r_3$};
\node (e4) at (2.5,-4) [circle,fill,inner sep=2pt] {$e_4$};
\draw [->] (r1) -- (e1);
\draw [->] (r2) -- (e2);
\draw [->] (r3) -- (e4);
\end{tikzpicture}
\end{center}

\begin{center}
\begin{tabular}{cccccc}
0 & 1 & 1 & 1 & 1 & 1 \\
0 & 0 & 2 & 3 & 3 & 5 \\
0 & 0 & 0 & 4 & 4 & \\
\end{tabular}
\end{center}

\[t: 0 \quad 1 \quad 2 \quad 3 \quad 4 \quad 5\]
Global Counter Array Simplification

\[ G \]

\[ \begin{array}{cccccc}
0 & 1 & 1 & 1 & 1 & 1 \\
0 & 0 & 2 & 3 & 3 & 5 \\
0 & 0 & 0 & 0 & 4 & 4 \\
\end{array} \]

\[ t: \] 0 1 2 3 4 5
Experiment Setup

Environment

- VM
- Ubuntu 18.04
- 4 GB RAM

---

6https://github.com/504ensicsLabs/LiME
7https://github.com/volatilityfoundation/volatility
8Pagani, Fedorov, and Balzarotti 2019
Experiment Setup

Environment

- VM
- Ubuntu 18.04
- 4 GB RAM

Tools

- LiME \(^6\)
- Volatility \(^7\)

---

\(^6\)https://github.com/504ensicsLabs/LiME
\(^7\)https://github.com/volatilityfoundation/volatility
\(^8\)Pagani, Fedorov, and Balzarotti 2019
Experiment Setup

Environment

- VM
- Ubuntu 18.04
- 4 GB RAM

Tools

- LiME
- Volatility

Consistency indicators

- Local counters & global counter array in pivot program

---

6 https://github.com/504ensicsLabs/LiME
7 https://github.com/volatilityfoundation/volatility
8 Pagani, Fedorov, and Balzarotti 2019
Experiment Setup

Environment

- VM
- Ubuntu 18.04
- 4 GB RAM

Consistency indicators

- Local counters & global counter array in pivot program
- VMA count comparison\(^8\)

Tools

- LiME \(^6\)
- Volatility \(^7\)

\(^6\)https://github.com/504ensicsLabs/LiME
\(^7\)https://github.com/volatilityfoundation/volatility
\(^8\)Pagani, Fedorov, and Balzarotti 2019
Procedure

1. Restart VM
2. Start pivot program
3. Take memory dump
4. Execute additional programs
5. Dump pivot heap

Load = high
System state = live

1 minute
Procedure

- Restart VM
- Start pivot program
- Take memory dump
- Execute additional programs
- Dump pivot heap

Load

- Low: One thread
Procedure

Load

- Low: One thread
- High: Eight threads

System states

- Frozen
- Live
Procedure

1. Restart VM
2. Start pivot program
3. Take memory dump
4. Execute additional programs
5. Dump pivot heap

Load
- Low: One thread
- High: Eight threads

System states
- Frozen
Procedure

1. Restart VM
2. Start pivot program
3. Take memory dump
4. Execute additional programs
5. Dump pivot heap

Load
- Low: One thread
- High: Eight threads

System states
- Frozen
- Live
<table>
<thead>
<tr>
<th>System State</th>
<th>Inconsistency type</th>
<th>Activity</th>
<th>Min</th>
<th>Max</th>
<th>Average</th>
<th>Affected dumps</th>
</tr>
</thead>
<tbody>
<tr>
<td>Live</td>
<td>Quasi-instantaneous</td>
<td>Low</td>
<td>0</td>
<td>3</td>
<td>0.8</td>
<td>5/10</td>
</tr>
<tr>
<td></td>
<td></td>
<td>High</td>
<td>0</td>
<td>37</td>
<td>13.8</td>
<td>7/10</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Low</td>
<td>0</td>
<td>1</td>
<td>0.1</td>
<td>1/10</td>
</tr>
<tr>
<td></td>
<td></td>
<td>High</td>
<td>3</td>
<td>7</td>
<td>4.9</td>
<td>9/9</td>
</tr>
<tr>
<td>VMA</td>
<td></td>
<td>Low</td>
<td>0</td>
<td>1</td>
<td>0.1</td>
<td>1/10</td>
</tr>
<tr>
<td></td>
<td></td>
<td>High</td>
<td>3</td>
<td>7</td>
<td>4.9</td>
<td>9/9</td>
</tr>
</tbody>
</table>
Discussion
### Inconsistencies and Fragmentation

<table>
<thead>
<tr>
<th>#</th>
<th>Inconsistencies</th>
<th>Range (in pages)</th>
<th>Distances $\leq 10$ pages</th>
<th>Max distance</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>37</td>
<td>224 575</td>
<td>61</td>
<td>103 122</td>
</tr>
<tr>
<td>2</td>
<td>30</td>
<td>423 245</td>
<td>47</td>
<td>79 613</td>
</tr>
<tr>
<td>3</td>
<td>21</td>
<td>141 591</td>
<td>20</td>
<td>54 774</td>
</tr>
<tr>
<td>4</td>
<td>17</td>
<td>150 635</td>
<td>33</td>
<td>53 319</td>
</tr>
<tr>
<td>5</td>
<td>16</td>
<td>267 028</td>
<td>44</td>
<td>82 596</td>
</tr>
<tr>
<td>6</td>
<td>15</td>
<td>79 296</td>
<td>85</td>
<td>71 215</td>
</tr>
<tr>
<td>7</td>
<td>2</td>
<td>99 921</td>
<td>81</td>
<td>55 761</td>
</tr>
<tr>
<td>8</td>
<td>0</td>
<td>82 526</td>
<td>76</td>
<td>62 653</td>
</tr>
<tr>
<td>9</td>
<td>0</td>
<td>12 132</td>
<td>75</td>
<td>3 170</td>
</tr>
<tr>
<td>10</td>
<td>0</td>
<td>4 431</td>
<td>97</td>
<td>2 665</td>
</tr>
</tbody>
</table>
Taking a Closer Look

Dump no. 1

First 93 list elements

List element with max counter

103 122 pages
Benefits

- Exact quantification & localization of inconsistencies
- Observe the influence of fragmentation
- Size of observed range flexible (possible adjustments)
- Influence fragmentation
- Influence position in physical address space
Benefits

- Exact quantification & localization of inconsistencies
Benefits

- Exact quantification & localization of inconsistencies
- Observe the influence of fragmentation
Benefits

- Exact quantification & localization of inconsistencies
- Observe the influence of fragmentation
- Size of observed range flexible
Benefits

- Exact quantification & localization of inconsistencies
- Observe the influence of fragmentation
- Size of observed range flexible

Possible adjustments

- Influence fragmentation
- Influence position in physical address space
Benefits

- Exact quantification & localization of inconsistencies
- Observe the influence of fragmentation
- Size of observed range flexible

Possible adjustments

- Influence fragmentation
Benefits

- Exact quantification & localization of inconsistencies
- Observe the influence of fragmentation
- Size of observed range flexible

Possible adjustments

- Influence fragmentation
- Influence position in physical address space
Conclusion
Summary

- Observation method works
  - Theoretical proof
  - Practical case study
Summary

- Observation method works
  - Theoretical proof
  - Practical case study
- Most memory dumps are not quasi-instantaneous
Summary

- Observation method works
  - Theoretical proof
  - Practical case study
- Most memory dumps are not quasi-instantaneous
- Benefits of deliberately placed consistency indicators
Future Work

- Influence position of pivot program
Future Work

- Influence position of pivot program
- Observe quasi-instantaneous consistency at a higher level

Thank you for your attention!
Future Work

• Influence position of pivot program
• Observe quasi-instantaneous consistency at a higher level
Future Work

- Influence position of pivot program
- Observe quasi-instantaneous consistency at a higher level
- Extensive tool evaluations

Thank you for your attention!
Future Work

- Influence position of pivot program
- Observe quasi-instantaneous consistency at a higher level
- Extensive tool evaluations
- Search for additional consistency indicators
Future Work

- Influence position of pivot program
- Observe quasi-instantaneous consistency at a higher level
- Extensive tool evaluations
- Search for additional consistency indicators

Thank you for your attention!
References


