Timeliner

“Tipped Off by Your Memory Allocator”: Device-Wide User Activity Sequencing from Android Memory Images

Rohit Bhatia, Brendan Saltaformaggio, Seung Jei Yang, Aisha Ali-Gombe, Xiangyu Zhang, Dongyan Xu, Golden G. Richard III
Importance of a Timeline

Crime Scene Reconstruction

"involves evaluating the context of a scene and the physical evidence found there in an effort to identify what occurred and in what order it occurred."

Call/Message database, Web browsing, Chat logs
Importance of a Timeline

Call/Message database, Web browsing, Chat logs

App Specific Logs

Coarse Grained Actions

Not a Device-Wide Timeline
Importance of a Device-Wide Timeline

Cyber crimes typically involve a variety of mobile apps, with complex sequencing of user-actions.

Need a Device-Wide solution to recover past user-actions that is not influenceable by the device-owner.

Netflix

Maps

Distracted Driving
Persistent storage is not enough to re-sequence a device-wide timeline.

Timeliner complements existing memory forensic techniques.
Activities as User-Actions

Activities are Android abstractions for a “single, focused thing a user can do.”

<table>
<thead>
<tr>
<th>Application</th>
<th>VoipActivity</th>
<th>RecordAudio</th>
<th>CameraActivity</th>
</tr>
</thead>
<tbody>
<tr>
<td>Signal</td>
<td>ConversationList</td>
<td>Conversation</td>
<td>ShareActivity</td>
</tr>
<tr>
<td>Dialer</td>
<td>InCallActivity</td>
<td>CallLogActivity</td>
<td>CallDetailActivity</td>
</tr>
<tr>
<td>Chase</td>
<td>AccountsActivity</td>
<td>TransferActivity</td>
<td>QuickDepositStart</td>
</tr>
<tr>
<td>Netflix</td>
<td>HomeActivity</td>
<td>SearchActivity</td>
<td>MovieDetails</td>
</tr>
</tbody>
</table>

Some Applications and a Few Example Activities
Activities As User-Actions

Activities are Android abstractions for a “single, focused thing a user can do”

Activity Lifecycle handled by ActivityManagerService which provides device-wide supervision
Activity Stack As A Solution?

No ordering available between different Activity Stacks

Activity Stacks contain the current state, and not the past state – which is what we want
Timeliner recovers Activities using key self-identifying data structures.

- MovieDetailsActivity
- PlayerActivity
- Launcher
- DialContactsActivity
- InCallActivity
Timeliner recovers Activities using key self-identifying data structures.

Infer ordering based on allocated locations in memory.
Residual Data Structures

MovieDetailsActivity

Activity Manager Service

Apps

Android
Residual Data Structures

MovieDetailsActivity

Activity Manager Service
Residual Data Structures

Field/Value Matches

Roots

MovieDetailsActivity

Apps Android

Activity Manager Service
Residual Data Structures

netflix.ui.MovieDetailsActivity

MovieDetailsActivity

Apps

Android

Activity Manager Service
“First-Available” Allocation

Memory Allocator

Size A

Size B

Size C

Memory dump

Launcher

DialContactsActivity

InCallActivity
Temporal Ordering From Spatial Ordering

\{ (r_1, a_1), (r_2, a_2), (r_3, a_3) \}

\{ (r_1, c_1), (r_2, c_2), (r_3, c_3) \}

\{ (r_1, b_1), (r_2, b_2), (r_3, b_3) \}

Memory Allocator
Temporal Ordering From Spatial Ordering

\[ \text{allPrecede}(e,f) = \{ r \mid (r,m) \in e \land (r,n) \in f \land \max(m) < \min(n) \} \]

\[ \text{anySucceed}(e,f) = \{ r \mid (r,m) \in e \land (r,n) \in f \land \max(m) > \min(n) \} \]
Pruning Erroneous Edges

Transition Graph

1)

MovieDetailsActivity

2)

PlayerActivity

3)

DialContactsActivity

4)

InCallActivity

Erroneous Edge
Pruning Erroneous Edges

Existing Allocation

MovieDetailsActivity

PlayerActivity

Transition Graph

Size A

Size B

Size C

Launcher

Memory dump

PlayerActivity

MovieDetailsActivity

Transition Graph
Pruning Erroneous Edges

Transition Graph

Existing Allocation

Erroneous Edge

MovieDetailsActivity

PlayerActivity

DialContactsActivity

Launcher

Size A

Size B

Size C
Pruning Erroneous Edges

Transition Graph

MovieDetailsActivity

PlayerActivity

DialContactsActivity

InCallActivity

Existing Allocation

Erroneous Edge

Memory dump

Size A

Size B

Size C

Launcher

1

2

3

4
Pruning Erroneous Edges

Existing Allocation

Erroneous Edge

MovieDetailsActivity

Min-Cut

PlayerActivity

Undirected Transition Graph

DialContactsActivity

InCallActivity

Launcher

Size A

Size B

Size C

Size A

Size B

Size C
Pruning Erroneous Edges

Transition Graph

- MovieDetailsActivity
- PlayerActivity
- InCallActivity
- DialContactsActivity
- Launcher
Global Ordering

![Transition Graph]

- **MovieDetailsActivity**
- **PlayerActivity**
- **Launcher**
- **DialContactsActivity**
- **InCallActivity**
Global Ordering

Transition Graph

- MovieDetailsActivity
- PlayerActivity
- Launcher
- DialContactsActivity
- InCallActivity

Topological Sort

- MovieDetailsActivity
- PlayerActivity
- Launcher
- DialContactsActivity
- InCallActivity

Local Orderings

- MovieDetailsActivity
- PlayerActivity
- Launcher
- DialContactsActivity
- InCallActivity
Global Ordering

Transition Graph

Topological Sort

Global Ordering

MovieDetailsActivity

PlayerActivity

Launcher

DialContactsActivity

InCallActivity

MovieDetailsActivity

PlayerActivity

Launcher

DialContactsActivity

InCallActivity
Garbage Collection

Garbage Collected Activity

Garbage Collection frees up prior runs, potentially causing a spatial disordering
Garbage Collection

- MovieDetailsActivity
- PlayerActivity
- Launcher
- DialContactsActivity
- InCallActivity

Size A
Size B
Size C

Other Allocations
Garbage Collection

Joinable Local Orderings do not end in Garbage Collected Activities

Period of Garbage Collection
Active Usage: 41-50 minutes
Idle: 98-112 minutes
# Micro-Benchmarks

## Samsung S4 (Android 5.0)

<table>
<thead>
<tr>
<th>Test Sequence</th>
<th># of Activity Ordered</th>
<th># Of Paths</th>
<th>Ground Truth Distance</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>16</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>B</td>
<td>14</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>C</td>
<td>12</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>D</td>
<td>14</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>E</td>
<td>15</td>
<td>1</td>
<td>0</td>
</tr>
</tbody>
</table>

## LG G3 (Android 5.1)

<table>
<thead>
<tr>
<th>Test Sequence</th>
<th># of Activity Ordered</th>
<th># Of Paths</th>
<th>Ground Truth Distance</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>15</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>B</td>
<td>14</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>G</td>
<td>15</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>D</td>
<td>12</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>E</td>
<td>14</td>
<td>1</td>
<td>0</td>
</tr>
</tbody>
</table>

## Moto G3 (Android 6.0)

<table>
<thead>
<tr>
<th>Test Sequence</th>
<th># of Activity Ordered</th>
<th># Of Paths</th>
<th>Ground Truth Distance</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>15</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>C</td>
<td>15</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>D</td>
<td>12</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>G</td>
<td>14</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>H</td>
<td>14</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>I</td>
<td>14</td>
<td>1</td>
<td>0</td>
</tr>
</tbody>
</table>

- **Recovered Activity Launched Before Test Sequence**
- **Accurate Results**
- **10 Test Sequences A-J**
Design Generality: Spyware Attack Investigation

Activity A

Broadcast X

Broadcast Y

Activity B

Transition Graph
Design Generality: Spyware Attack Investigation

- Communication Receiver
- Conversation Activity
- CallRecorder Receiver
- InCall Activity
- FrontCamera Activity
- VideoTime Receiver
- GmailCompose Activity
- StopRecording Receiver
- Camera Video Spying Service
- Camera Picture Spying Service
- Microphone Audio Spying Service

Transition Graph

SMS Spying Service
Call Spying Service
Design Generality: Extension to jemalloc

Android

<table>
<thead>
<tr>
<th>Size A</th>
<th>Size B</th>
<th>Size C</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bucket</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Slot</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Run</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

“First-Available”

mozjemalloc

<table>
<thead>
<tr>
<th>Bin</th>
<th>Region</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

“First-Available”
Initially, the driver is using the Google Maps Navigation app.
Conclusion

Timeliner re-sequences an Android user’s past actions, even for terminated applications.

Timeliner infers temporal ordering of Activities from memory layout of key self-identifying data structures.

Accurate reconstruction of various applicable crime scenarios and extension beyond user actions and Android.
Thank You!

Questions?

Rohit Bhatia
bhatia13@purdue.edu