OVRseen: Auditing Network Traffic and Privacy Policies in Oculus VR

31st USENIX Security Symposium
Aug 10-12, 2022 - Boston, MA, USA

Rahmadi Trimananda, Hieu Le, Hao Cui, Janice Tran Ho, Anastasia Shuba*, Athina Markopoulou

*Currently with DuckDuckGo. The work was done prior to Anastasia's joining DuckDuckGo and does not necessarily reflect the views of DuckDuckGo.
Virtual Reality (VR)

Zuckerberg sees virtual reality as next major computing platform

Facebook's CEO says the $2 billion acquisition of Oculus VR is about much more than gaming

Virtual Reality For Good Use Cases:
From Educating On Racial Bias To Pain Relief During Childbirth

THE VR IN THE ENTERPRISE REPORT: How retailers and brands are illustrating VR's potential in sales, employee training, and product development

Apparently, it's the next big thing. What is the metaverse?
Virtual Reality (VR)

Source: https://www.oculus.com/, https://attractionsmagazine.com/
Virtual Reality (VR)

Source: https://www.oculus.com/, https://attractionsmagazine.com/
Virtual Reality (VR)

- VR sensors may collect *body and motion data*:
  - movement,
  - play area, etc.

Source: https://www.oculus.com/, https://unity.com/
Virtual Reality (VR)

- **VR sensors may collect** body and motion data:
  - movement,
  - play area, etc.

- **On-device ads are coming!**
  - immersive,
  - use sensory and biometrics info

Source: https://www.oculus.com/, https://unity.com/
Virtual Reality (VR)

- VR sensors may collect body and motion data:
  - movement,

VR is the next **BIG THING**, but

- its **privacy** implications are **not** well understood yet
  - immersive,
  - use sensory and biometrics info

Source: https://www.oculus.com/, https://unity.com/
Outline

- Intro to VR
Outline

● Intro to VR
● Related Work & Our Approach
Related Work

Website

Mobile

Smart TV

Voice Assistants

Smart Home

VR
Related Work

[Degeling et. al., NDSS'19]
Website

[Enck et. al., OSDI'10]
Mobile

[Shuba et. al., PETS'18]

[Moghaddam et. al., CCS'19]
Smart TV

[Trimananda et. al., NDSS'20]
Voice Assistants

[Ren et. al., IMC'19]
Smart Home

[Shuba et. al., PETS'18]

[Varmarken et. al., PETS'20]
VR
Related Work

- Website: [Degeling et. al., NDSS'19]
- Mobile: [Enck et. al., OSDI'10], [Shuba et. al., PETS'18]
- Smart TV: [Moghaddam et. al., CCS'19]
- Voice Assistants: [Trimananda et. al., NDSS'20], [Ren et. al., IMC'19]
- Smart Home: [Lentzsch et. al., NDSS'21], [Shuba et. al., PETS’18]
- VR: [Varmarken et. al., PETS’20], [Degeling et. al., NDSS’19], [Lentzsch et. al., NDSS’21]

- User study: [Adams et. al., SOUPS’18]
- Body motion data analysis: [Miller et. al., Nature’20]
Our Approach: **Auditing Traffic & Policy**
Our Approach: Auditing Traffic & Policy

Network Traffic

App  App  ...  App

Platform

First-party
Platform-party
Third-party

VR
Our Approach: **Auditing Traffic & Policy**

Network Traffic

- App
- App
- ... App
- Platform

- First-party
- Platform-party
- Third-party

Privacy Policy

- Policies
- GDPR
- California Consumer Privacy Act

VR

---

ProperData

UCI University of California, Irvine
Our Approach: Auditing Traffic & Policy

Network Traffic

First-party
Platform-party
Third-party

Consistency

Privacy Policy

First-party
Platform-party
Third-party
Our Approach: Auditing Traffic & Policy

Network Traffic

App ➔ App ➔ ... ➔ App

Platform

First-party
Platform-party
Third-party

Information flow
Transmission Principle
sender, data type, recipient, [subject]; purpose, other

Privacy Policy

Source: https://www.libroworld.com/
Our Approach: Auditing Traffic & Policy

Network Traffic

App  App  ...  App
Platform

First-party
Platform-party
Third-party

<sender, data type, recipient, [subject]; purpose, other>
Our Approach: Auditing Traffic & Policy

Network Traffic

App  App  ...  App

Platform

First-party
Platform-party
Third-party

<sender, data type, recipient, purpose>

Privacy Policy

GDPR

California Consumer Privacy Act
Our Approach: **Auditing Traffic & Policy**

Network Traffic

- First-party
- Platform-party
- Third-party

<sender, data type, recipient, purpose>

Privacy Policy

Beat Saber Privacy Policy
Our Approach: Auditing Traffic & Policy

Network Traffic

Platform

<beat_saber, user_id, beat_games, functionality>

<sender, data type, recipient, purpose>

Privacy Policy

Beat Saber Privacy Policy
Our Approach: **Auditing Traffic & Policy**

**Network Traffic**

- **Platform**
  - First-party
  - Platform-party
  - Third-party

- `<beat_saber, user_id, beat_games, functionality>`
- `<sender, data type, recipient, purpose>`
- `<beat_saber, user_id, beat_games, functionality>`
Our Approach: **Auditing Traffic & Policy**

1. Data flows from **traffic**
2. Collection statements from **policy**
3. **Consistency** between the two
Our Approach: Auditing Traffic & Policy

(1) Data flows from traffic
(2) Collection statements from policy
(3) Consistency between the two
Outline

- Intro to VR
- Related Work & Our Approach
Outline

- Intro to VR
- Related Work & Our Approach
- OVRseen
  - Network Traffic
Network Traffic

Network Traffic Analysis

App Stores

- oculus
- SIDEQUEST
Network Traffic

Network Traffic Analysis

App Stores
- oculus
- SIDEQUEST

Start with 150 most popular apps
Network Traffic

Network Traffic Analysis

Network Traffic Collection

App Stores

App

Oculus Quest 2
Network Traffic

Network Traffic Analysis

Network Traffic Collection

VPN-based decryption tool with no rooting
Network Traffic

Network Traffic Analysis

Network Traffic Collection

App Stores

oculus
SIDEQUEST

App
FRIDA Agent
AntMonitor
FRIDA Client Libraries

Certificate validation bypass
Network Traffic Analysis

Network Traffic Collection

**App Stores**
- oculus
- SIDEQUEST

**App**
- FRIDA Agent

**AntMonitor**
- FRIDA Client Libraries

**Challenge #1: Decryption**
- JVM-based techniques for Frida
  - Function found through symbol table
- Stripped binary on Oculus OS
Network Traffic

Network Traffic Analysis

Network Traffic Collection
- App
- FRIDA Agent
- AntMonitor

Raw Data
- PCAPNG
- JSON

Trace post-processing

App Stores
- oculus
- SIDEQUEST
Network Traffic Analysis

Network Traffic Collection

App Stores

App

FRIDA Agent

AntMonitor

FRIDA Client Libraries

Raw Data

PCAPNG

JSON

Data Flows

App

Data Type

Destination

Data flow extraction

<app, data type, destination>
Network Traffic: Collection Results

Network Traffic Analysis

Network Traffic Collection
- App Stores: Oculus, SideQuest
- App
- FRIDA Agent
- AntMonitor
- FRIDA Client Libraries

Raw Data
- PCAPNG
- JSON

Data Flows
- App
- Data Type
- Destination

<table>
<thead>
<tr>
<th>App Store</th>
<th>Apps</th>
<th>Domains</th>
<th>eSLDs</th>
<th>Packets</th>
<th>TCP Fl.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Oculus-Free</td>
<td>43</td>
<td>85</td>
<td>48</td>
<td>2,818</td>
<td>2,126</td>
</tr>
<tr>
<td>Oculus-Paid</td>
<td>49</td>
<td>54</td>
<td>35</td>
<td>2,278</td>
<td>1,883</td>
</tr>
<tr>
<td>SideQuest</td>
<td>48</td>
<td>57</td>
<td>40</td>
<td>2,679</td>
<td>2,260</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td>140</td>
<td>158</td>
<td>92</td>
<td>7,775</td>
<td>6,269</td>
</tr>
</tbody>
</table>
Network Traffic: Collection Results

Network Traffic Collection

App Stores
- oculus
- SIDEQUEST

App
FRIDA Agent
AntMonitor

FRIDA Client Libraries

Raw Data
- PCAPNG
- JSON

Data Flows
- App
- Data Type
- Destination

<table>
<thead>
<tr>
<th>App Store</th>
<th>Apps</th>
<th>Domains</th>
<th>eSLDs</th>
<th>Packets</th>
<th>TCP Fl.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Oculus-Free</td>
<td>43</td>
<td>85</td>
<td>48</td>
<td>2,818</td>
<td>2,126</td>
</tr>
<tr>
<td>Oculus-Paid</td>
<td>49</td>
<td>54</td>
<td>35</td>
<td>2,278</td>
<td>1,883</td>
</tr>
<tr>
<td>SideQuest</td>
<td>48</td>
<td>57</td>
<td>40</td>
<td>2,679</td>
<td>2,260</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>140</strong></td>
<td><strong>158</strong></td>
<td><strong>92</strong></td>
<td><strong>7,775</strong></td>
<td><strong>6,269</strong></td>
</tr>
</tbody>
</table>
## Network Traffic: Collection Results

### Network Traffic Analysis

### Network Traffic Collection

- **App Stores**
  - Oculus
  - SIDEQUEST

- **FRIDA Agent**
  - AntMonitor

- **FRIDA Client Libraries**

- **Raw Data**
  - PCAPNG
  - JSON

- **Data Flows**
  - App
  - Data Type
  - Destination

### Network Traffic: Collection Results

<table>
<thead>
<tr>
<th>App Store</th>
<th>Apps</th>
<th>Domains</th>
<th>eSLDs</th>
<th>Packets</th>
<th>TCP Fl.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Oculus-Free</td>
<td>43</td>
<td>85</td>
<td>48</td>
<td>2,818</td>
<td>2,126</td>
</tr>
<tr>
<td>Oculus-Paid</td>
<td>49</td>
<td>54</td>
<td>35</td>
<td>2,278</td>
<td>1,883</td>
</tr>
<tr>
<td>SideQuest</td>
<td>48</td>
<td>57</td>
<td>40</td>
<td>2,679</td>
<td>2,260</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td>140</td>
<td>158</td>
<td>92</td>
<td><strong>7,775</strong></td>
<td><strong>6,269</strong></td>
</tr>
</tbody>
</table>

UCI University of California, Irvine
Network Traffic

App Stores

Network Traffic Collection

FRIDA Agent

F R I D A Client Libraries

App

Network Traffic Analysis

Raw Data

PCAPNG

JSON

Data Flows

App

Data Type

Destination

Data Types Exposures

Data types analysis
### Network Traffic: Data Types Found

<table>
<thead>
<tr>
<th>Data Types (21)</th>
<th>1st Apps</th>
<th>3rd Apps Pl.</th>
<th>1st FQDNs</th>
<th>3rd FQDNs Pl.</th>
<th>% Blocked 1st</th>
<th>% Blocked 3rd</th>
</tr>
</thead>
<tbody>
<tr>
<td>PII Device ID</td>
<td>6</td>
<td>64</td>
<td>2</td>
<td>6</td>
<td>13</td>
<td>1</td>
</tr>
<tr>
<td>User ID</td>
<td>5</td>
<td>65</td>
<td>0</td>
<td>5</td>
<td>13</td>
<td>0</td>
</tr>
<tr>
<td>Android ID</td>
<td>6</td>
<td>31</td>
<td>18</td>
<td>6</td>
<td>7</td>
<td>2</td>
</tr>
<tr>
<td>Serial Number</td>
<td>0</td>
<td>0</td>
<td>18</td>
<td>0</td>
<td>0</td>
<td>2</td>
</tr>
<tr>
<td>Person Name</td>
<td>1</td>
<td>7</td>
<td>0</td>
<td>1</td>
<td>4</td>
<td>0</td>
</tr>
<tr>
<td>Email</td>
<td>2</td>
<td>5</td>
<td>0</td>
<td>2</td>
<td>5</td>
<td>0</td>
</tr>
<tr>
<td>Geolocation</td>
<td>0</td>
<td>5</td>
<td>0</td>
<td>0</td>
<td>4</td>
<td>0</td>
</tr>
</tbody>
</table>

### Fingerprint

<table>
<thead>
<tr>
<th>Data Types</th>
<th>1st</th>
<th>2nd</th>
<th>3rd</th>
<th>4th</th>
<th>5th</th>
<th>6th</th>
<th>7th</th>
<th>8th</th>
<th>9th</th>
</tr>
</thead>
<tbody>
<tr>
<td>SDK Version</td>
<td>23</td>
<td>69</td>
<td>20</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Hardware Info</td>
<td>21</td>
<td>65</td>
<td>19</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>System Version</td>
<td>16</td>
<td>62</td>
<td>19</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Session Info</td>
<td>7</td>
<td>66</td>
<td>2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>App Name</td>
<td>4</td>
<td>65</td>
<td>2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Build Version</td>
<td>0</td>
<td>61</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Flags</td>
<td>6</td>
<td>53</td>
<td>2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Usage Time</td>
<td>2</td>
<td>59</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Language</td>
<td>5</td>
<td>28</td>
<td>16</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cookies</td>
<td>5</td>
<td>4</td>
<td>2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### VR Sensory Data

<table>
<thead>
<tr>
<th>Data Types</th>
<th>1st</th>
<th>2nd</th>
<th>3rd</th>
<th>4th</th>
<th>5th</th>
<th>6th</th>
<th>7th</th>
<th>8th</th>
<th>9th</th>
</tr>
</thead>
<tbody>
<tr>
<td>VR Play Area</td>
<td>0</td>
<td>40</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>VR Movement</td>
<td>1</td>
<td>24</td>
<td>2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>VR Field of View</td>
<td>0</td>
<td>16</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>VR Pupillary</td>
<td>0</td>
<td>16</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

| Total            | 33  | 70  | 22  | 44  | 39  | 5   | 36  | 20  |

---

The table above summarizes the data types found in network traffic analysis of App Stores, highlighting specific fields such as device IDs, user IDs, Android IDs, and serial numbers. The Fingerprint section details various SDK versions and other data types, while the VR Sensory Data section focuses on virtual reality play areas and movement. The total count provides a comprehensive overview of the data types encountered, indicating 40 unique data types.
## Network Traffic: Data Types Found

### Data Types (21)

**PII**
- Device ID
- User ID
- Android ID
- Serial Number
- Person Name
- Email
- Geolocation

**Fingerprint**
- SDK Version
- Hardware Info
- System Version
- Session Info
- App Name
- Build Version
- Flags
- Usage Time
- Language
- Cookies

**VR Sensory Data**
- VR Play Area
- VR Movement
- VR Field of View
- VR Pupillary Distance

### Data Types Found
21 data types: PII, Fingerprint, etc.
## Network Traffic: Data Types Found

### Data Types (21)

<table>
<thead>
<tr>
<th>Data Type</th>
<th>1st Apps</th>
<th>3rd Apps</th>
<th>Pl.</th>
<th>1st FQDNs</th>
<th>3rd FQDNs</th>
<th>Pl.</th>
<th>% Blocked</th>
<th>1st</th>
<th>3rd</th>
<th>Pl.</th>
</tr>
</thead>
<tbody>
<tr>
<td>PII</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Device ID</td>
<td>6</td>
<td>64</td>
<td>2</td>
<td>6</td>
<td>13</td>
<td>1</td>
<td>0</td>
<td>38</td>
<td>100</td>
<td></td>
</tr>
<tr>
<td>User ID</td>
<td>5</td>
<td>65</td>
<td>0</td>
<td>5</td>
<td>13</td>
<td>0</td>
<td>20</td>
<td>38</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Android ID</td>
<td>6</td>
<td>31</td>
<td>18</td>
<td>6</td>
<td>7</td>
<td>2</td>
<td>17</td>
<td>43</td>
<td>50</td>
<td></td>
</tr>
<tr>
<td>Serial Number</td>
<td>0</td>
<td>0</td>
<td>18</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>-</td>
<td>-</td>
<td>50</td>
<td></td>
</tr>
<tr>
<td>Person Name</td>
<td>1</td>
<td>7</td>
<td>0</td>
<td>1</td>
<td>4</td>
<td>0</td>
<td>0</td>
<td>50</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Email</td>
<td>2</td>
<td>5</td>
<td>0</td>
<td>2</td>
<td>5</td>
<td>0</td>
<td>0</td>
<td>20</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Geolocation</td>
<td>0</td>
<td>5</td>
<td>0</td>
<td>0</td>
<td>4</td>
<td>0</td>
<td>-</td>
<td>50</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Fingerprint</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SDK Version</td>
<td>23</td>
<td>69</td>
<td>20</td>
<td>34</td>
<td>28</td>
<td>4</td>
<td>6</td>
<td>46</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>Hardware Info</td>
<td>21</td>
<td>65</td>
<td>19</td>
<td>25</td>
<td>23</td>
<td>3</td>
<td>4</td>
<td>39</td>
<td>33</td>
<td></td>
</tr>
<tr>
<td>System Version</td>
<td>16</td>
<td>62</td>
<td>19</td>
<td>20</td>
<td>21</td>
<td>3</td>
<td>5</td>
<td>43</td>
<td>33</td>
<td></td>
</tr>
<tr>
<td>Session Info</td>
<td>7</td>
<td>66</td>
<td>2</td>
<td>7</td>
<td>13</td>
<td>1</td>
<td>14</td>
<td>46</td>
<td>100</td>
<td></td>
</tr>
<tr>
<td>App Name</td>
<td>4</td>
<td>65</td>
<td>2</td>
<td>4</td>
<td>10</td>
<td>1</td>
<td>25</td>
<td>40</td>
<td>100</td>
<td></td>
</tr>
<tr>
<td>Build Version</td>
<td>0</td>
<td>61</td>
<td>0</td>
<td>0</td>
<td>3</td>
<td>0</td>
<td>0</td>
<td>100</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Flags</td>
<td>6</td>
<td>53</td>
<td>2</td>
<td>6</td>
<td>8</td>
<td>1</td>
<td>0</td>
<td>50</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Usage Time</td>
<td>2</td>
<td>59</td>
<td>0</td>
<td>0</td>
<td>4</td>
<td>0</td>
<td>0</td>
<td>100</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Language</td>
<td>5</td>
<td>28</td>
<td>16</td>
<td>5</td>
<td>8</td>
<td>0</td>
<td>0</td>
<td>36</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cookies</td>
<td>5</td>
<td>4</td>
<td>2</td>
<td>0</td>
<td>4</td>
<td>0</td>
<td>0</td>
<td>33</td>
<td>100</td>
<td></td>
</tr>
<tr>
<td>VR Sensory Data</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>VR Play Area</td>
<td>0</td>
<td>40</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>-</td>
<td>100</td>
<td></td>
<td></td>
</tr>
<tr>
<td>VR Movement</td>
<td>1</td>
<td>24</td>
<td>2</td>
<td>1</td>
<td>6</td>
<td>1</td>
<td>0</td>
<td>67</td>
<td>100</td>
<td></td>
</tr>
<tr>
<td>VR Field of View</td>
<td>0</td>
<td>16</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>-</td>
<td>100</td>
<td></td>
<td></td>
</tr>
<tr>
<td>VR Pupillary</td>
<td>0</td>
<td>16</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>-</td>
<td>100</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Distance</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Total</td>
<td>33</td>
<td>70</td>
<td>22</td>
<td>44</td>
<td>39</td>
<td>5</td>
<td>5</td>
<td>36</td>
<td>20</td>
<td></td>
</tr>
</tbody>
</table>

- **21 data types:** PII, Fingerprint, and VR-specific types.
Network Traffic Analysis

Network Traffic Collection

App Stores
- oculus
- SIDEQUEST

App
- FRIDA Agent
- AntMonitor

FRIDA Client Libraries

Raw Data
- PCAPNG
- JSON

Data Flows
- App
- Data Type
- Destination

Data Types Exposures

Data types analysis
Network Traffic

Network Traffic Analysis

Network Traffic Collection
- App Stores
  - Oculus
  - SIDEQUEST
- App
- FRIDA Agent
- AntMonitor

FRIDA Client Libraries

Raw Data
- PCAPNG
- JSON

Data Flows
- App
- Data Type
- Destination

Network Traffic Analysis
- Data Types Exposures
- ATS Ecosystem

ATS analysis

44
Network Traffic Analysis

Network Traffic Collection

Raw Data

Data Flows

Network Traffic Analysis

Data Types Exposures

ATS Ecosystem

App Stores

App

Frida Client Libraries

AntMonitor

Network Traffic:

ATS Found

Network Traffic Analysis

ATS Ecosystem

Facebook

Facebook-Hardware

Oculus

Oculus CDN

Unity 3D

Google

Google APIs

Google Analytics

Cloud Functions

Mixpanel

Graph Facebook Hardware

Graph Oculus

Scontent Oculus CDN

Config UCA Cloud Unity 3D

CDP Cloud Unity 3D

Perf Events Cloud Unity 3D

Example

API Mixpanel

Yurapp 502de Firebase App

www Google Analytics

Network Traffic Analysis

ATS Ecosystem

Facebook

Facebook Hardware

Oculus

Oculus CDN

Unity 3D

Google

Google APIs

Google Analytics

Cloud Functions

Mixpanel

Graph Facebook Hardware

Graph Oculus

Scontent Oculus CDN

Config UCA Cloud Unity 3D

CDP Cloud Unity 3D

Perf Events Cloud Unity 3D

Example

API Mixpanel

Yurapp 502de Firebase App

www Google Analytics

eSLD

ATS FQDN

Number of Apps

Third-party

Platform-party

Number of Apps

Third-party

Platform-party

Network Traffic Analysis

App Stores

AntMonitor

Frida Client Libraries

Network Traffic Collection

Raw Data

Data Flows

Network Traffic Analysis

Data Types Exposures

ATS Ecosystem

Facebook

Facebook Hardware

Oculus

Oculus CDN

Unity 3D

Google

Google APIs

Google Analytics

Cloud Functions

Mixpanel

Graph Facebook Hardware

Graph Oculus

Scontent Oculus CDN

Config UCA Cloud Unity 3D

CDP Cloud Unity 3D

Perf Events Cloud Unity 3D

Example

API Mixpanel

Yurapp 502de Firebase App

www Google Analytics

eSLD

ATS FQDN

Number of Apps

Third-party

Platform-party

Number of Apps

Third-party

Platform-party

Network Traffic Analysis

App Stores

AntMonitor

Frida Client Libraries

Network Traffic Collection

Raw Data

Data Flows

Network Traffic Analysis

Data Types Exposures

ATS Ecosystem

Facebook

Facebook Hardware

Oculus

Oculus CDN

Unity 3D

Google

Google APIs

Google Analytics

Cloud Functions

Mixpanel

Graph Facebook Hardware

Graph Oculus

Scontent Oculus CDN

Config UCA Cloud Unity 3D

CDP Cloud Unity 3D

Perf Events Cloud Unity 3D

Example

API Mixpanel

Yurapp 502de Firebase App

www Google Analytics

eSLD

ATS FQDN

Number of Apps

Third-party

Platform-party

Number of Apps

Third-party

Platform-party

Network Traffic Analysis

App Stores

AntMonitor

Frida Client Libraries

Network Traffic Collection

Raw Data

Data Flows

Network Traffic Analysis

Data Types Exposures

ATS Ecosystem

Facebook

Facebook Hardware

Oculus

Oculus CDN

Unity 3D

Google

Google APIs

Google Analytics

Cloud Functions

Mixpanel

Graph Facebook Hardware

Graph Oculus

Scontent Oculus CDN

Config UCA Cloud Unity 3D

CDP Cloud Unity 3D

Perf Events Cloud Unity 3D

Example

API Mixpanel

Yurapp 502de Firebase App

www Google Analytics

eSLD

ATS FQDN

Number of Apps

Third-party

Platform-party

Number of Apps

Third-party

Platform-party

Network Traffic Analysis

App Stores

AntMonitor

Frida Client Libraries

Network Traffic Collection

Raw Data

Data Flows

Network Traffic Analysis

Data Types Exposures

ATS Ecosystem

Facebook

Facebook Hardware

Oculus

Oculus CDN

Unity 3D

Google

Google APIs

Google Analytics

Cloud Functions

Mixpanel

Graph Facebook Hardware

Graph Oculus

Scontent Oculus CDN

Config UCA Cloud Unity 3D

CDP Cloud Unity 3D

Perf Events Cloud Unity 3D

Example

API Mixpanel

Yurapp 502de Firebase App

www Google Analytics

eSLD

ATS FQDN

Number of Apps

Third-party

Platform-party

Number of Apps

Third-party

Platform-party

Network Traffic Analysis

App Stores

AntMonitor

Frida Client Libraries

Network Traffic Collection

Raw Data

Data Flows

Network Traffic Analysis

Data Types Exposures

ATS Ecosystem

Facebook

Facebook Hardware

Oculus

Oculus CDN

Unity 3D

Google

Google APIs

Google Analytics

Cloud Functions

Mixpanel

Graph Facebook Hardware

Graph Oculus

Scontent Oculus CDN

Config UCA Cloud Unity 3D

CDP Cloud Unity 3D

Perf Events Cloud Unity 3D

Example

API Mixpanel

Yurapp 502de Firebase App

www Google Analytics

eSLD

ATS FQDN

Number of Apps

Third-party

Platform-party

Number of Apps

Third-party

Platform-party

Network Traffic Analysis

App Stores

AntMonitor

Frida Client Libraries

Network Traffic Collection

Raw Data

Data Flows

Network Traffic Analysis

Data Types Exposures

ATS Ecosystem

Facebook

Facebook Hardware

Oculus

Oculus CDN

Unity 3D

Google

Google APIs

Google Analytics

Cloud Functions

Mixpanel

Graph Facebook Hardware

Graph Oculus

Scontent Oculus CDN

Config UCA Cloud Unity 3D

CDP Cloud Unity 3D

Perf Events Cloud Unity 3D

Example

API Mixpanel

Yurapp 502de Firebase App

www Google Analytics

eSLD

ATS FQDN

Number of Apps

Third-party

Platform-party

Number of Apps

Third-party

Platform-party

Network Traffic Analysis

App Stores

AntMonitor

Frida Client Libraries

Network Traffic Collection

Raw Data

Data Flows

Network Traffic Analysis

Data Types Exposures

ATS Ecosystem

Facebook

Facebook Hardware

Oculus

Oculus CDN

Unity 3D

Google

Google APIs

Google Analytics

Cloud Functions

Mixpanel

Graph Facebook Hardware

Graph Oculus

Scontent Oculus CDN

Config UCA Cloud Unity 3D

CDP Cloud Unity 3D

Perf Events Cloud Unity 3D

Example

API Mixpanel

Yurapp 502de Firebase App

www Google Analytics

eSLD

ATS FQDN

Number of Apps

Third-party

Platform-party

Number of Apps

Third-party

Platform-party

Network Traffic Analysis

App Stores

AntMonitor

Frida Client Libraries

Network Traffic Collection

Raw Data

Data Flows

Network Traffic Analysis

Data Types Exposures

ATS Ecosystem

Facebook

Facebook Hardware

Oculus

Oculus CDN

Unity 3D

Google

Google APIs

Google Analytics

Cloud Functions

Mixpanel

Graph Facebook Hardware

Graph Oculus

Scontent Oculus CDN

Config UCA Cloud Unity 3D

CDP Cloud Unity 3D

Perf Events Cloud Unity 3D

Example

API Mixpanel

Yurapp 502de Firebase App

www Google Analytics

eSLD

ATS FQDN

Number of Apps

Third-party

Platform-party

Number of Apps

Third-party

Platform-party

Network Traffic Analysis

App Stores

AntMonitor

Frida Client Libraries

Network Traffic Collection

Raw Data

Data Flows

Network Traffic Analysis

Data Types Exposures

ATS Ecosystem

Facebook

Facebook Hardware

Oculus

Oculus CDN

Unity 3D

Google

Google APIs

Google Analytics

Cloud Functions

Mixpanel

Graph Facebook Hardware

Graph Oculus

Scontent Oculus CDN

Config UCA Cloud Unity 3D

CDP Cloud Unity 3D

Perf Events Cloud Unity 3D

Example

API Mixpanel

Yurapp 502de Firebase App

www Google Analytics

eSLD

ATS FQDN

Number of Apps

Third-party

Platform-party

Number of Apps

Third-party

Platform-party
Network Traffic Analysis

Network Traffic Collection

App

FRIDA Client Libraries

AntMonitor

Raw Data

PCAPNG

JSON

Data Flows

App

Data Type

Destination

Network Traffic Analysis

Data Types

Exposures

ATS Ecosystem

App Stores

oculus

SIDEQUEST

facebook.com

facebook-hardware.com

oculus.com

oculuscdn.com

unity3d.com

graph.facebook-hardware.com

graph.oculus.com

scontent.oculuscdn.com

config.uca.cloud.unity3d.com

cdp.cloud.unity3d.com

google.com

gooleapis.com

google-analytics.com

cloudfunctions.net

mixpanel.com

Number of Apps

Number of Apps
Network Traffic

Network Traffic Analysis

Network Traffic Collection

- FRIDA Client Libraries
- PCAPNG
- JSON

Raw Data

- App
- Data Type
- Destination

Data Flows

- Network Traffic Analysis
  - Data Types Exposures
  - ATS Ecosystem

App Stores

- oculus
- SIDEQUEST

AntMonitor

FRIDA Agent

App

ProperData

UCI University of California, Irvine
Network Traffic Analysis

Network Traffic Collection

App
FRIDA Agent
AntMonitor
FRIDA Client Libraries

Raw Data
PCAPNG
JSON

Data Flows
App
Data Type
Destination

Network Traffic Analysis
Data Types Exposures
ATS Ecosystem

Data Flows In Context
App
Data Type
Destination

Context
Purpose
Other
Network Traffic Analysis: **Key Takeaways**

### Network Traffic Collection
- **App Stores**
  - oculus
  - SIDEQUEST

- **FRIDA Client Libraries**
- **AntMonitor**

- **PCAPNG**
- **JSON**

### Raw Data
- **App**
- **Data Type**
- **Destination**

### Data Analysis
- **Data Types**
- **Exposures**
- **ATS Ecosystem**

#### Young ATS ecosystem
- 21 data types
- Social/analytics tracking domains
- No on-device ads (yet)

---

*ProperData UCI University of California, Irvine*
Outline

- Intro to VR
- Related Work & Our Approach
- OVRseen
  - Network Traffic
Outline

● Intro to VR
● Related Work & Our Approach
● OVRseen
  ○ Network Traffic
  ○ Privacy Policy
Privacy Policy

App Stores
- oculus
- SIDEQUEST

Privacy Policy Analysis

& Third Parties

oculus

& Third Parties
Privacy Policy

App Stores
- oculus
- SIDEQUEST

Privacy Policy Analysis

Privacy Policies

Privacy policies from first-, platform-, and third-party
Privacy Policy

27% apps did not provide a policy.

Privacy Policy Analysis

Privacy Policies
Privacy Policy

Network Traffic Analysis

Data Flows
- App
- Data Type
- Destination

Privacy Policy Analysis

Privacy Policies

Privacy Policy Analyzer

Collection Statements
- App
- Data Type
- Entity

Automated policy analysis

App Stores
- oculus
- SIDEQUEST

& Third Parties
- oculus
- &

App Stores
- oculus
- SIDEQUEST

& Third Parties
- oculus
- &
App Stores

Privacy Policy: Contribution

Challenge #2: Policy Analysis
- [PoliCheck, SEC'20]
- [Polisis, SEC'18]
- [OVRseen, SEC'22]: Adapted for VR

Privacy Policy Analysis

Privacy Policy Analyzer

Collection Statements
- App
- Data Type
- Entity
# Privacy Policy

## Network Traffic Analysis

![Network Traffic Analysis Diagram]

<table>
<thead>
<tr>
<th>Field</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version</td>
<td>4</td>
</tr>
<tr>
<td>IHL</td>
<td>8</td>
</tr>
<tr>
<td>TOS</td>
<td>16</td>
</tr>
<tr>
<td>Total length</td>
<td>31 bit</td>
</tr>
<tr>
<td>Identification</td>
<td></td>
</tr>
<tr>
<td>Flags</td>
<td></td>
</tr>
<tr>
<td>Fragment offset</td>
<td></td>
</tr>
<tr>
<td>TTL</td>
<td></td>
</tr>
<tr>
<td>Protocol</td>
<td></td>
</tr>
<tr>
<td>Header checksum</td>
<td></td>
</tr>
<tr>
<td>Source IP: Device/App address</td>
<td></td>
</tr>
<tr>
<td>Destination IP: Beat Games address</td>
<td></td>
</tr>
</tbody>
</table>

App Stores
- oculus
- SIDEQUEST

## Privacy Policy Analysis

**Beat Saber Privacy Policy**

1. **Who are you?**
2. **1.1. We are Beat Games**
3. **3. What kind of personal data about me are you collecting and why?**
4. **3.1. So that you can play Beat Saber and we are able to repair and improve the game, we collect the following data about you:**
   - Identification data (Avatar, nickname or UserID under which you are registered, etc.);
   - Technical data (data about your device etc.);
   - Data concerning your use of Beat Saber (when and how and how successfully you play the game).
   - We only use these personal data for the two below-specified purposes:
     - To enable the functioning of Beat Saber and to create statistics contributing to the improvement of the game.
Privacy Policy

Network Traffic Analysis

<table>
<thead>
<tr>
<th>Version</th>
<th>IHL</th>
<th>TOS</th>
<th>Total length</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- TTL
- Protocol
- Header checksum

- Source IP: Device/App address
- Destination IP: Beat Games address

Options

Data

{ user_id, ... }

App Stores

- oculus
- SIDEQUEST

Privacy Policy Analysis

Beat Saber Privacy Policy

1. Who are you?
1.1. We are Beat Games

3. What kind of personal data about me are you collecting and why?
3.1. So that you can play Beat Saber and we are able to repair and improve the game, we collect the following data about you:
- Identification data (Avatar, nickname or UserID under which you are registered, etc.);
- Technical data (data about your device etc.);
- Data concerning your use of Beat Saber (when and how and how successfully you play the game).

We only use these personal data for the two below-specified purposes:
- To enable the functioning of Beat Saber and to create statistics contributing to the improvement of the game.
**Privacy Policy**

**Network Traffic Analysis**

- **App Stores**
  - oculus
  - SIDEQUEST

- **BEAT SABER**

**Privacy Policy Analysis**

**Beat Saber Privacy Policy**

1. Who are you?
2. We are Beat Games.
3. What kind of personal data about me are you collecting and why?
4. So that you can play Beat Saber and we are able to repair and improve the game, we collect the following data about you:
   - identification data (Avatar, nickname or UserID under which you are registered, etc.);
   - technical data (data about your device etc.);
   - data concerning your use of Beat Saber (when and how and how successfully you play the game).
5. We only use these personal data for the two below-specified purposes:
   - to enable the functioning of Beat Saber and to create statistics contributing to the improvement of the game.
**Network Traffic Analysis**

<table>
<thead>
<tr>
<th>0</th>
<th>4</th>
<th>8</th>
<th>16</th>
<th>31 bit</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version</td>
<td>IHL</td>
<td>TOS</td>
<td>Total length</td>
<td>Identification</td>
</tr>
<tr>
<td>TTL</td>
<td>Protocol</td>
<td>Header checksum</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Source IP: Device/App address</td>
<td>Destination IP: Beat Games address</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Options</td>
<td>Data</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>{ user_id, ... }</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- **App Stores**
  - oculus
  - SIDEQUEST

- **PoliCheck**

**Privacy Policy Analysis**

Beat Saber Privacy Policy

1. Who are you?
   1.1. We are Beat Games

3. What kind of personal data about you are we collecting and why?
   3.1. So that you can play Beat Saber and we are able to repair and improve the game, we collect the following data about you:
      - identificaiton data (Avatar, nickname or UserID under which you are registered, etc.);
      - technical data (data about your device etc.);
      - data concerning your use of Beat Saber (when and how and how successfully you play the game).

We only use these personal data for the two below-specified purposes:
- to enable the functioning of Beat Saber and to create statistics contributing to the improvement of the game.
Privacy Policy

Network Traffic Analysis

<table>
<thead>
<tr>
<th>Version</th>
<th>IHL</th>
<th>TOS</th>
<th>Total length</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Identification</th>
<th>Flags</th>
<th>Fragment offset</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source IP: Device/App address</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Destination IP: Beat Games address</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>TTL</th>
<th>Protocol</th>
<th>Header checksum</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Options</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data</td>
</tr>
</tbody>
</table>

{ user_id, ... }

Source IP: Device/App address

App Stores

○ oculus
○ SIDEQUEST

Privacy Policy Analysis

Beat Saber Privacy Policy

1. Who are you?
   1.1. We are Beat Games

3. What kind of personal data about me are you collecting and why?
   3.1. So that you can play Beat Saber and we are able to repair and improve the game, we collect the following data about you:
   - Identification data (Avatar, nickname or email under which you are registered, etc.); technical data (data about your device etc.);
   - data concerning your use of Beat Saber (when and how and how successfully you play the game).
   - We only use these personal data for the two below-specified purposes:
   - to enable the functioning of Beat Saber and to create statistics contributing to the improvement of the game.

PoliCheck
App Stores

 LIABILITY

 Privacy Policy Analysis

 Beat Saber Privacy Policy

 1. Who are you?
 2. We are Beat Games
 3. What kind of personal data about me are you collecting and why?
 3.1. So that you can play Beat Saber and we are able to repair and improve the game, we collect the following data about you:
 identification data (Avatar, nickname or ServerId under which you are registered, etc.);
 technical data (data about your device etc.);
 data concerning your use of Beat Saber (when and how and how successfully you play the game).
 We only use these personal data for the two below-specified purposes:
 to enable the functioning of Beat Saber and to create statistics contributing to the improvement of the game.
Privacy Policy

21 data types

1. Who are you?
1.1. We are Beat Games

3. What kind of personal data about me are you collecting and why?
3.1. So that you can play Beat Saber and we are able to repair and improve the game, we collect the following data about you:
- identification data (Avatar, nickname or UserID under which you are registered, etc.);
- technical data (data about your device etc.);
- data concerning your use of Beat Saber (when and how and how successfully you play the game).

We only use these personal data for the two below-specified purposes:
- to enable the functioning of Beat Saber and
- to create statistics contributing to the improvement of the game.
Privacy Policy

1. Who are you?
1.1. We are Beat Games:

3. What kind of personal data about me are you collecting and why?
3.1. So that you can play Beat Saber and we are able to repair and improve the game, we collect the following data about you:
identification data (Avatar, nickname or UserID under which you are registered, etc.);
technical data (data about your device etc.);
data concerning your use of Beat Saber (when and how and how successfully you play the game).
We only use these personal data for the two below specified purposes:
to enable the functioning of Beat Saber and to create statistics contributing to the improvement of the game.
Privacy Policy

1. Who are you?
1.1. We are Beat Games

3. What kind of personal data about me are you collecting and why?
3.1. So that you can play Beat Saber and we are able to repair and improve the game, we collect the following data about you:
- Identification data (Avatar, nickname or UserID under which you are registered, etc.);
- Technical data (data about your device etc.);
- Data concerning your use of Beat Saber (when and how and how successfully you play the game).

We only use these personal data for the two below specified purposes:
- to enable the functioning of Beat Saber and to create statistics contributing to the improvement of the game.
- Other

Privacy Policy Analyzer

Data Ontology

Collection Statements

App

Data Type

Entity

Ontology for data types
Privacy Policy

Network Traffic Analysis

- Data Flows
  - App Stores
  - Network Traffic Collection
    - AntMonitor
    - Agent
    - Client
    - Libraries
  - Raw Data
    - PCAPNG
    - JSON

Network Traffic Analysis

- Data Types
  - Exposures
  - ATS
  - Ecosystem

Privacy Policy Analysis

- & Third Parties
  - Privacy Policies
  - Privacy Policy Analyzer
  - Data Ontology
    - Entity Ontology
      - Collection Statements
        - App
        - Data Type
        - Entity

Ontology for destination entities
Privacy Policy

<table>
<thead>
<tr>
<th>Platform</th>
<th>Data Ontology</th>
<th>Entity Ontology</th>
</tr>
</thead>
<tbody>
<tr>
<td>Android [5]</td>
<td>38 nodes</td>
<td>209 nodes</td>
</tr>
<tr>
<td>OVR (OVRSEEN)</td>
<td>62 nodes</td>
<td>64 nodes</td>
</tr>
<tr>
<td>New nodes in OVR</td>
<td>39 nodes</td>
<td>21 nodes</td>
</tr>
</tbody>
</table>

Privacy Policy Analyzer

Data Ontology

Collection Statements

App

Data Type

Entity

Entity Ontology

Adapted from Android
Privacy Policy

Network Traffic Analysis

Network Traffic Collection

App Stores

App

RIFA

Agent

AntMonitor

FRIDA Client Libraries

Raw Data

PCAPNG

JSON

Data Flows

Data Types

Exposures

Network Traffic Analysis

Data Type

Destination

ATS Ecosystem

Data Flows In Context

App

Data Type

Destination

Privacy Policy Analysis

Privacy Policies

Data Ontology

Collection Statements

Entity Ontology

App

Data Type

Entity

Context

App

Data Type

Destination

& Third Parties

Policies

Data Ontology

Collection Statements

Entity Ontology
Privacy Policy

Network Traffic Analysis

Network Traffic Collection
- App
- FRIDA Client Libraries
- AntMonitor

Raw Data
- PCAPNG
- JSON

Data Flows
- App
- Data Type
- Destination

Network Traffic Analysis
- Data Types
- Exposures
- ATS Ecosystem

App Stores
- oculus
- SIDEQUEST

Privacy Policy Analysis

Privacy Policies
- Policies

Privacy Policy Analyzer
- Data Ontology
- Entity Ontology
- Collection Statements
- Improved PoliCheck

Context
- Data flows vs. collection statements

Improved PoliCheck

Data flows vs. collection statements

Data Flows In Context
- App
- Data Type
- Destination
Privacy Policy: Consistency Results

Data Flows
- App
- Data Type
- Destination

Collection Statements
- App
- Data Type
- Entity

Improved PoliCheck

Network-to-policy consistency

Entity Ontology
- ProperData
- UCI University of California, Irvine
Privacy Policy: Consistency Results

70% inconsistent
Fingerprint + VR Sensory Data
Privacy Policy: Consistency Results

No referencing platform + third party

70% inconsistent Fingerprint + VR Sensory Data
Privacy Policy: Consistency Results

70% inconsistent
Fingerprint + VR Sensory Data

Referencing platform + third party
74% consistent
Privacy Policy: Key Takeaways

- Developers' privacy policies
  - Missing!
  - Poorly written
  - Neglect referencing third-party policies

Referencing platform + third party
74% consistent

70% inconsistent
Fingerprint + VR Sensory Data
Privacy Policy

PoliCheck + Polisis

<sender, data type, recipient, purpose>
Privacy Policy

PoliCheck + Polisis

sender, data type, recipient, purpose

Data Flows
- App
- Data Type
- Destination

Collection Statements
- App
- Data Type
- Purpose

Improved PoliCheck
- Translation
- Polisis

Context
- Consistency
- Purpose

Entity Ontology

Privacy Policy Analyzer

Data Ontology
- Entity Ontology

Privacy Policies
- ATS Ecosystem
- Exposures
- Network Traffic Analysis
- PCAPNG
- JSON
- Client Libraries

& Third Parties

Privacy Policies

PoliCheck + Polisis

<sender, data type, recipient, purpose>
Privacy Policy

PoliCheck + Polisis

<sender, data type, recipient, purpose>

Data Flows
- App
- Data Type
- Destination

Collection Statements
- Improved PoliCheck
- Translation
- Polisis

Entity Ontology
- Data Type
- Polisis

Context
- Consistency
- Purpose

Exposures
- ATS
- Ecosystem

Privacy Policy Analyzer
- Privacy Policies
- Polsis

AntMonitor
- Agent
- PCAPNG
- JSON

Client Libraries
- Third Parties

Privacy Policies & Third Parties

App Store
- Network Traffic Collection
- App Data Flows

Data Types
- Exposure
- Polisis

Purpose
- Polisis

Complex Decision Extraction
Privacy Policy

PoliCheck + Polisis

<s sender, data type, recipient, purpose>

69% non-core func.
31% core functionality

App Stores
Raw Data
Network Traffic Collection
App Data Flows
App Data Type
Destination
Network Traffic Analysis
Data Types
Exposures
ATS
Ecosystem
AntMonitor
Agent
PCAPNG
JSON
Client
Libraries

Privacy Policies

Privacy Policy Analyzer
Data Ontology
Entity Ontology
Collection Statements
Improved PoliCheck
Translation
Context
Consistency
Purpose

PoliCheck + Polisis

<sender, data type, recipient, purpose>

69% non-core func.
31% core functionality
Outline

● Intro to VR
● Related Work & Our Approach
● OVRseen
  ○ Network Traffic
  ○ Privacy Policy
● Conclusions
OVRseen

- Auditing privacy in VR
  - Network traffic
  - Privacy policy
OVRseen

- Auditing privacy in VR
  - Network traffic
  - Privacy policy

- 21 data types including VR Sensory Data
- Young, centralized, and ad-free ecosystem
OVRseen

- Auditing privacy in VR
  - Network traffic
  - Privacy policy

- 21 data types including VR Sensory Data
- Young, centralized, and ad-free ecosystem

- 27% apps did not provide a policy
- 70% data flows are inconsistent
  - 74% consistent when referencing platform and third-party
- 69% data flows are for non-core functionality
OVRseen

- Auditing privacy in VR
  - Network traffic
  - Privacy policy

- 21 data types including VR Sensory Data
- Young, centralized, and ad-free ecosystem

- 27% apps did not provide a policy
- 70% data flows are inconsistent
  - 74% consistent when referencing platform and third-party
- 69% data flows are for non-core functionality

Responsible disclosure: 24 developers responded
Thank you!

Code and datasets available
https://athinagroup.eng.uci.edu/projects/ovrseen/
https://properdata.eng.uci.edu/

rtrimana@uci.edu / properdata@uci.edu
Recommendations

- Developers to provide privacy policy that
  - references other parties' privacy policy
  - provides notice and ask for consent

- Notifying platform + developers
  - Oculus + 140 developers
  - 24 developers responded: 21 were positive
Network Traffic

Network Traffic Analysis

Network Traffic Collection

App Stores

App

FRIDA Agent

AntMonitor

FRIDA Client Libraries

Run JS code to control Frida Agent
Network Traffic Analysis

Network Traffic Collection

AntMonitor

FRIDA Agent

FRIDA Client Libraries

Run JS code to control Frida Agent

● Stripped binary vs. JVM
Network Traffic

- Stripped binary vs. JVM
- Find cert. validation function

Network Traffic Analysis

Network Traffic Collection

App

F RIDA Agent

AntMonitor

Run JS code to control Frida Agent

App Stores

oculus

SIDEQUEST

F RIDA Client Libraries

Libraries

Client

93
Network Traffic

Network Traffic Analysis

Network Traffic Collection

- Stripped binary vs. JVM
- Find cert. validation function
  - Find Unity version in APK

Run JS code to control Frida Agent

App Stores

- oculus
- SIDEQUEST
Network Traffic

Network Traffic Analysis

Network Traffic Collection

App Stores

- oculus
- SIDEQUEST

App

FRIDA Agent

AntMonitor

FRIDA Client Libraries

Run JS code to control Frida Agent

- Stripped binary vs. JVM
- Find cert. validation function
  - Find Unity version in APK
  - Download the symbolicated library
Network Traffic

Network Traffic Analysis

Network Traffic Collection

App Stores
- oculus
- SIDEQUEST

App
FRIDA Agent

AntMonitor
FRIDA Client Libraries

Run JS code to control Frida Agent

- Stripped binary vs. JVM
- Find cert. validation function
  - Find Unity version in APK
  - Download the symbolicated library
  - Find the cert. val. function address
Network Traffic

Network Traffic Analysis

Network Traffic Collection

- Stripped binary vs. JVM
- Find cert. validation function
  - Find Unity version in APK
  - Download the symbolicated library
  - Find the cert. val. function address
  - Extract binary pattern

Run JS code to control Frida Agent
Network Traffic

Network Traffic Analysis

Network Traffic Collection

- App
- App Stores
- AntMonitor

Frida Agent

Frida Libraries

Stripped binary vs. JVM

- Find cert. validation function
  - Find Unity version in APK
  - Download the symbolicated library
  - Find the cert. val. function address
  - Extract binary pattern
  - Find pattern in APK

Run JS code to control Frida Agent
Network Traffic

Network Traffic Analysis

Network Traffic Collection

App Stores

Frida Agent

Run JS code to control Frida Agent

- Stripped binary vs. JVM
- Find cert. validation function
  - Find Unity version in APK
  - Download the symbolicated library
  - Find the cert. val. function address
  - Extract binary pattern
  - Find pattern in APK

```c
3229  /* Verify the certificate validity (user-chosen profile, not restartable)
3230  */
3231  int mbedtls_x509_crt_verify_with_profile( mbedtls_x509_crt *crt,
3232      mbedtls_x509_crt *trust_ca,
3233      mbedtls_x509_crl *ca_crl,
3234      const mbedtls_x509_crt_profile *profile,
3235      const char *cn, uint32_t *flags,
3236      int (*e_vrfy)(void *, mbedtls_x509_crt *, int, uint32_t *),
3237      void (*vrfy) )
3238  {
3239  
3240      return mbedtls_x509_crt_verify_restartable_ca_cb( crt, trust_ca, ca_crl,
3241          NULL, NULL,
3242          profile, cn, flags,
3243          f_vrfy, p_vrfy, NULL ) ;
3244  }
```

https://github.com/Mbed-TLS/mbedtls/blob/development/library/x509_crt.c
Network Traffic

Network Traffic Analysis

Network Traffic Collection

App Stores

oculus

SIDEQUEST

App

FRIDA Agent

AntMonitor

FRIDA Client Libraries

Run JS code to control Frida Agent

- Stripped binary vs. JVM
- Find cert. validation function
  - Find Unity version in APK
  - Download the symbolicated library
  - Find the cert. val. function address
  - Extract binary pattern
  - Find pattern in APK
- Intercept

https://github.com/Mbed-TLS/mbedtls/blob/development/library/x509_crt.c
Network Traffic Analysis

Network Traffic Collection

App
FRIDA Agent
FRIDA Client
Libraries
AntMonitor

Run JS code to control Frida Agent

- Stripped binary vs. JVM
- Find cert. validation function
  - Find Unity version in APK
  - Download the symbolicated library
  - Find the cert. val. function address
  - Extract binary pattern
  - Find pattern in APK
- Intercept
- Change return value

```c
/* Verify the certificate validity (user-chosen profile, not restartable) */
int mbedtls_x509_crt_verify_with_profile( mbedtls_x509_crt *crt,
                                        mbedtls_x509_crt *trust_ca,
                                        mbedtls_x509_crl *ca_crl,
                                        mbedtls_x509_crl_profile *profile,
                                        const char *ca, uint32_t *flags,
                                        void (*e_vrfy)(void *, mbedtls_x509_crt *, int, uint32_t *) );

return( mbedtls_x509_crt_verify_restartable_ca_cb( crt, trust_ca, ca_crl, 0 );
```

https://github.com/Mbed-TLS/mbedtls/blob/development/library/x509_crt.c
Network Traffic Analysis

Network Traffic Collection

- Stripped binary vs. JVM
- Find cert. validation function
  - Find Unity version in APK
  - Download the symbolicated library
  - Find the cert. val. function address
  - Extract binary pattern
  - Find pattern in APK
- Intercept
- Change return value

Run JS code to control Frida Agent

- Find cert. validation function
  - Find Unity version in APK
  - Download the symbolicated library
  - Find the cert. val. function address
  - Extract binary pattern
  - Find pattern in APK

https://github.com/Mbed-TLS/mbedtls/blob/development/library/x509_crt.c
1. Who are you?

1.1. We are Beat Games

3. What kind of personal data about me are you collecting and why?

3.1. So that you can play Beat Saber and we are able to repair and improve the game, we collect the following data about you:

- Identification data (Avatar, nickname or user id under which you are registered, etc.);
- Technical data (data about your device, etc.);
- Data concerning your use of Beat Saber (when and how and how successfully you play the game).

We only use these personal data for the two below-specified purposes:

- To enable the functioning of Beat Saber and to create statistics contributing to the improvement of the game.

Traffic: <beat_saber, user_id, beat_games>

Policy: <beat_saber, user_id, beat_games>
1. Who are you?
1.1. We are Beat Games

3. What kind of personal data about me are you collecting and why?
3.1. So that you can play Beat Saber and we are able to repair and improve the game, we collect the following data about you:
identification data (Avatar, nickname or \texttt{UserId} under which you are registered, etc.);
technical data (data about your device, etc.); data concerning your use of Beat Saber (when and how and how successfully you play the game).

We only use these personal data for the two below-specified purposes:
to enable the functioning of Beat Saber and to create statistics contributing to the improvement of the game.

Traffic: \texttt{<beat_saber, user_id, beat_games>}
Policy: \texttt{<beat_saber, user_id, beat_games>}

Privacy Policy Analyzer

Data Ontology
Collection Statements
App
Data Type
Entity

Ontology for data types
<table>
<thead>
<tr>
<th>Disclosure Type</th>
<th>Privacy Policy Text</th>
<th>Action : Data Collection Statement (P)</th>
<th>Data Flow (F)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Clear</td>
<td>“For example, we collect information ..., and a timestamp for the request.”</td>
<td>collect : ( \langle \text{com.cvr.terminus, usage time, we} \rangle )</td>
<td>( \langle \text{usage time, we} \rangle )</td>
</tr>
<tr>
<td>Vague</td>
<td>“We will share your information (in some cases personal information) with third-parties, ...”</td>
<td>collect : ( \langle \text{com.HomeNetGames.WW1oculus, pii, third party} \rangle )</td>
<td>( \langle \text{serial number, oculus} \rangle ), ( \langle \text{android id, oculus} \rangle )</td>
</tr>
<tr>
<td>Omitted</td>
<td>-</td>
<td>collect : ( \langle \text{com.kluge.SynthRiders, -, -} \rangle )</td>
<td>( \langle \text{system version, oculus} \rangle ), ( \langle \text{sdk version, oculus} \rangle ), ( \langle \text{hardware information, oculus} \rangle )</td>
</tr>
<tr>
<td>Ambiguous</td>
<td>“..., Skydance will not disclose any Personally Identifiable Information to third parties ... your Personally Identifiable Information will be disclosed to such third parties and ...”</td>
<td>collect : ( \langle \text{com.SDI.TWD, pii, third party} \rangle )</td>
<td>( \langle \text{serial number, oculus} \rangle ), ( \langle \text{android id, oculus} \rangle )</td>
</tr>
<tr>
<td>Incorrect</td>
<td>“We do not share our customer’s personal information with unaffiliated third parties ...”</td>
<td>not_collect : ( \langle \text{com.downpourinteractive. onward, pii, third party} \rangle )</td>
<td>( \langle \text{device id, unity} \rangle ), ( \langle \text{user id, oculus} \rangle )</td>
</tr>
</tbody>
</table>
Privacy Policy

Consistent Disclosure
Clear

Traffic: <beat_saber, user_id, beat_games>
Policy: <beat_saber, user_id, beat_games>

Exact match

Data Flows
- App
- Data Type
- Destination

Privacy Policy Analyzer
- Data Ontology
- Collection Statements
- Improved PoliCheck
- Entity Ontology
- Entity

Network-to-policy consistency

Context Consistency
Privacy Policy

Consistent Disclosure
Vague

Traffic: <beat_saber, device_id, beat ...>
Policy: <beat_saber, technical_data, ...>

Policy uses generic term

Data Flows
- App
- Data Type
- Destination

Privacy Policy Analyzer
- Data Ontology
- Collection Statements
- Improved PoliCheck
- Entity Ontology
- Entity

Context
Consistency
Network-to-policy consistency
Inconsistent Disclosure
Omitted

Traffic: <beat_saber, user_id, beat_games>
Policy: <N/A>

Policy has no statement
Privacy Policy

**Inconsistent Disclosure**

**Ambiguous**

Traffic: `<beat_saber, user_id, beat_games>`

Policy: `<beat_saber, user_id, beat_games> collect`

`<beat_saber, user_id, beat_games> not_col`

Policy has conflicting statements

Network-to-policy consistency
Privacy Policy

Inconsistent Disclosure

Incorrect

Traffic: `<beat_saber, user_id, beat_games>`

Policy: `<beat_saber, user_id, beat_games>` not_col

Policy has false statements

Improved PoliCheck

Network-to-policy consistency

Context

Consistency