AML: Matching SMS with HTTPS

Henning Schmidtpott
Integrierte Leitstelle Freiburg · Breisgau-Hochschwarzwald (ILS)
Emergency Control Center Freiburg, Germany
Emergency call handling in Germany

• Two national emergency numbers:
  • 112: Fire and rescue, emergency medical services
  • 110: Police

• 16 federal states
  • 233 PSAPs handling 112 calls
Emergency control center Freiburg

- Population ≈ 500,000
- 112 calls/year ≈ 100,000
- Integrated in main fire station
- Own data center
AML endpoint Germany

• The national AML endpoint is provided by Freiburg Emergency Control Center since 2019.
• Redundancy endpoint in Berlin (passive).
• Over 230 PSAPs have access to AML endpoint.
• 60,000 HTTPS messages per day from Android devices.
• 80,000 SMS messages per day from Android and iOS devices.
• 3 messages per call (after 0s, 15s, 30s).
Integration in PSAP application
Integration in PSAP application
Statistics

Mobile emergency calls received by PSAP in Freiburg with AML location in %
AML in a privacy friendly way

• Delete all data on the endpoint after 1 hour
• Refuse not necessary data like IMSI, device model, ...
• device number is only stored as hash value in database
Location data flow
Location data process
Access to location data by API

• PSAP starts request to AML endpoint
• caller number as request parameter
• AML endpoint sends answer with location data for the requested caller number back to PSAP

=> Correct device number is significant!
# Security issues with HTTPS?

<table>
<thead>
<tr>
<th>risk</th>
<th>measure</th>
</tr>
</thead>
<tbody>
<tr>
<td>Malicious code injection, SQL injection</td>
<td>Check ELS data for compatibility. Refuse incompatible data. Examples:</td>
</tr>
<tr>
<td></td>
<td>Characters in device_number may only include numbers and plus (e.g. +49171234567890)</td>
</tr>
<tr>
<td></td>
<td>Characters in location_latitude may only include a dot(.) and numbers (e.g. 7.364758).</td>
</tr>
<tr>
<td>DDoS attack</td>
<td>General practice like server redundancy, monitoring, use backbone protection from provider, isolate HTTPS-Server from SMS-Server</td>
</tr>
<tr>
<td>Fake/prank data</td>
<td>No problem unless the ELS data is associated to a real emergency call.</td>
</tr>
</tbody>
</table>
Matching HTTPS and SMS

• Use device_imei as key
## Example dataset

### HTTPS

<table>
<thead>
<tr>
<th>location_time</th>
<th>device_number</th>
<th>location_latitude</th>
<th>location_longitude</th>
<th>location_accuracy</th>
<th>location_altitude</th>
<th>device_languages</th>
<th>device_imei</th>
</tr>
</thead>
<tbody>
<tr>
<td>2022-06-28 15:00:00</td>
<td>0</td>
<td>49.654321</td>
<td>7.123456</td>
<td>29</td>
<td>129</td>
<td>de-DE,pl-PL</td>
<td>35249411446</td>
</tr>
</tbody>
</table>

### SMS

<table>
<thead>
<tr>
<th>location_time</th>
<th>device_number</th>
<th>location_latitude</th>
<th>location_longitude</th>
<th>location_accuracy</th>
<th>location_altitude</th>
<th>device_languages</th>
<th>device_imei</th>
</tr>
</thead>
<tbody>
<tr>
<td>2022-06-28 15:00:00</td>
<td>b81a97f74e8e15190c</td>
<td>49.654321</td>
<td>7.123456</td>
<td>29</td>
<td></td>
<td></td>
<td>35249411446</td>
</tr>
</tbody>
</table>

### HTTPS & SMS after merge

<table>
<thead>
<tr>
<th>location_time</th>
<th>device_number</th>
<th>location_latitude</th>
<th>location_longitude</th>
<th>location_accuracy</th>
<th>location_altitude</th>
<th>device_languages</th>
<th>device_imei</th>
</tr>
</thead>
<tbody>
<tr>
<td>2022-06-28 15:00:00</td>
<td>b81a97f74e8e15190c</td>
<td>49.654321</td>
<td>7.123456</td>
<td>29</td>
<td>129</td>
<td>de-DE,pl-PL</td>
<td>35249411446</td>
</tr>
</tbody>
</table>
Roaming

• HTTPS is an easy solution to provide AML for roaming caller.
• Data volume is very small so the costs are not significant.
• About 5% of all HTTPS datasets we receive are from roaming caller.