Shared Signals and Events

Fall 2020 Update

Atul Tulshibagwale (Google)
Tim Cappalli (Microsoft)
What is SSE?

- Synchronize distributed state relating to shared principals
  - Users
  - Authentication
  - Devices
  - ...more in future
- Profile of Security Event Tokens (SETs)
- Using an asynchronous publish and subscribe method
### Applications of Shared Signals and Events

<table>
<thead>
<tr>
<th>Continuous Access Evaluation Protocol (CAEP)</th>
<th>RISC</th>
</tr>
</thead>
<tbody>
<tr>
<td>● Conveys state changes relating to access to resources</td>
<td>● Enables providers to prevent attackers from compromising linked accounts</td>
</tr>
<tr>
<td>● Enables peers to tune access to updated state</td>
<td>● RISC helps enables coordination in restoring accounts in the event of compromise</td>
</tr>
<tr>
<td>● Event types include:</td>
<td>● Event types include:</td>
</tr>
<tr>
<td>○ Credential change</td>
<td>○ Account purged</td>
</tr>
<tr>
<td>○ Token claims change</td>
<td>○ Credential change required</td>
</tr>
<tr>
<td>○ Level of Assurance change</td>
<td>○ Identifier recycled</td>
</tr>
<tr>
<td>○ Device compliance change</td>
<td></td>
</tr>
</tbody>
</table>
Progress Since Spring 2020

- First draft of SSE Profile of SETs spec published in May
- Virtual Workshop hosted by Google in June
  - Attended by Google, Microsoft, Cisco, Thales, Sailpoint, VMWare, Intuit, Target and others
- Results from Workshop:
  - Go forward on draft spec
  - Start work on CAEP Event types spec
- Re-worked spec to depend on IETF SecEvents Subject Identifiers draft
Outline of Changes to SSE Spec

- Subject Principals and SPAGs
  - Entities managed by Transmitters and Receivers
  - Referenced by Subjects in SSE events
  - Subject Principal Administrative Groupings (SPAGs) represent collections of Subject Principals

- Transmitter Status Changes
  - Status may be queried and updated for specific SPAGs
  - Authorization per SPAG update request
CAEP Event Type Examples

- **Current Event Types**
  - **Session Revoked**
  - **Token Claims Change** (ex: location or IP address change)
  - **Credential Change** (ex: user added a FIDO2 authenticator)
  - **Device Compliance Change** (ex: device was compliant and is now not compliant)
  - **Assurance Level Change** (ex: LoA increased or decreased for a user or device)

- Event types do not mandate specific subject identifiers
- Custom claims allowed between transmitter and receiver
[Example] Session Revoked: User + Device

```json
{
"iss": "https://login.microsoftonline.com/e69e17d9-8a93-4156-bed8-71036f23080d/",
"jti": "24c63fb56e5a2d77a6b512616ca9fa24",
"iat": 1600976590,
"aud": "https://events.workspace.google.com/caep",
"events": {
  "https://schemas.openid.net/secevent/caep/event-type/session-revoked": {
    "subject_type": "user-device",
    "user": {
      "subject_type": "iss-sub",
      "iss": "https://login.microsoftonline.com/e69e17d9-8a93-4156-bed8-71036f23080d/",
      "sub": "jane.smith@example.com"
    },
    "device": {
      "subject_type": "iss-sub",
      "iss": "https://login.microsoftonline.com/e69e17d9-8a93-4156-bed8-71036f23080d/",
      "sub": "e9297990-14d2-42ec-a4a9-4036db86509a"
    }
  },
  "initiating_entity": "policy",
  "reason_admin": "Policy Violation: C076E82F",
  "reason_user": "Your device is no longer compliant.",
  "tenant_id": "123456789",
  "event_timestamp": 1600975810
}
}```