STAR: Distributed Secret Sharing for Threshold Aggregation Reporting

PPM WG, IETF 116

Shivan Sahib
Idea: k-anonymity for clients reporting measurements to an untrusted server
Goals

- **Cheap**: low computational overhead and network usage for clients and servers
- **Simple**: easy to implement, well-known crypto
- **Private**: practical privacy guarantees for the client
Client wants to send a telemetry value to the server, but only wants the server to see it if there are $\geq K$ submissions of the same value.
Implementations

- Shipping in Brave browser for telemetry
- Rust (Shamir): https://github.com/brave/sta-rs
- Rust (verifiable + benchmarks): https://github.com/claucece/secret-sharing-extra
- Go (verifiable + benchmarks): https://github.com/chris-wood/star-go/
- WASM bindings: https://github.com/brave/sta-rs/tree/main/star-wasm
<table>
<thead>
<tr>
<th>Secret Sharing Scheme</th>
<th>Signature Scheme/Protocol</th>
<th>Client threat mitigated</th>
</tr>
</thead>
<tbody>
<tr>
<td>Shamir Secret Sharing</td>
<td>OPRF</td>
<td>None</td>
</tr>
<tr>
<td>Verifiable Secret Sharing</td>
<td>OPRF</td>
<td>Bad shares (DoS)</td>
</tr>
<tr>
<td>Shamir Secret Sharing</td>
<td>Blind Signatures</td>
<td>Bad ciphertext</td>
</tr>
<tr>
<td>Verifiable Secret Sharing</td>
<td>Blind Signatures</td>
<td>Both</td>
</tr>
</tbody>
</table>
- There seems to be strong interest in STAR
- We addressed feedback from the WG and it improved the document
- We should do this formally within the WG!