Capsule: A Protocol for Secure Collaborative Document Editing

Nadim Kobeissi
We’ve all been there…

Plan to conquer the world
<table>
<thead>
<tr>
<th>Capsule: Security Goals</th>
</tr>
</thead>
<tbody>
<tr>
<td>Participant List Integrity.</td>
</tr>
<tr>
<td>Confidentiality.</td>
</tr>
<tr>
<td>Integrity.</td>
</tr>
<tr>
<td>Authentication.</td>
</tr>
<tr>
<td>Transcript Consistency.</td>
</tr>
</tbody>
</table>
Capsule: Simple, Elegant Protocol

- Document is a *hash chain of diffs*.
- Access to document is obtained by sharing a simple ID.
- Users must prove knowledge of ID to participate in document.
- Primitives:
  - BLAKE2 for symmetric operations.
  - Ed25519 for signatures.
Capsule: Formally Verified

Protocol Level
- Formally verified with ProVerif.
- Hand proof.

Implementation Level
- HACL-WASM: First software to use HACL* in WebAssembly.
- Functional correctness, secure memory, no side channels.
Capsule: Amazing!

• An open standard that anyone can use.
• Learn more: https://symbolic.software/capsule/
• ePrint paper: https://eprint.iacr.org/2018/253
• Email me! nadim@symbolic.software