Encrypted Collaborative Real-Time Document Editing

Kevin Körner, Robert Finze, Thomas Walter

24.09.2015, Tübingen
What is Real-Time Document Editing?
Existing Products
Well-known collaborative real-time editors

• Google Docs (today Google Drive)
• Microsoft OneDrive
• Etherpad
• Edupad

• Microsoft announcement: RTCE in Office 2016
Problem Description

Client 1

RTCE-Server

Clients 2 - n

- Manages document updating
- Loads and stores document from/to persistent storage
- Manages accessing Clients

RTCE-Server requires lots of trust!
• Keep the RTCE idea without trusting the RTE-Server

• RTCE-Server should not
  - know the documents content
  - know which changes were made by the accessing clients
  - interact with the persistent storage
  - not accidentally leak information

• RTCE-Server should
  - store an operations list
  - Define an order of performed operations
  - validate accessing clients autorisation
Solution
Secure RTCE-System

Clients 2 - n

ID | Encrypted
---|---------
1  | Ba(3$rvj
2  |
3  |
4  |
5  |
Client 1

Hello World!

RTCE-Server

Clients 2 - n

ID | Encrypted
---|------------
1  | Ba(3$rvj
2  |            
3  |            
4  |            
5  |            

Solution
Secure RTCE-System

Hello World
Solution
Secure RTCE-System

Client 1
Hello World!

Enc(Op(add,!,11),K_S)

RTCE-Server

Clients 2 - n

Hello World

<table>
<thead>
<tr>
<th>ID</th>
<th>Encrypted</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Ba(3$rvj)</td>
</tr>
<tr>
<td>2</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td></td>
</tr>
</tbody>
</table>
Solution
Secure RTCE-System

Hello World

Clients 2 - n

Client 1

Hello World!

Enc(Op(add, !11), K_S)

ID | Encrypted
---|---
1  | Ba(3$rvj
2  | 
3  | 
4  | 
5  | 

Hello World!
Solution
Secure RTCE-System

- Clients 2 - n

- Client 1
  - Hello World!

- RTCE-Server

- Enc(\text{Op}\langle \text{add},!,11 \rangle,K_S)

<table>
<thead>
<tr>
<th>ID</th>
<th>Encrypted</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>\text{Ba}(3$rvj</td>
</tr>
<tr>
<td>2</td>
<td>(?js%mwP</td>
</tr>
<tr>
<td>3</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td></td>
</tr>
</tbody>
</table>
Client 1
Hello World!

RTCE-Server

Clients 2 - n

ID was 2

Hello World

<table>
<thead>
<tr>
<th>ID</th>
<th>Encrypted</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Ba(3$rvj</td>
</tr>
<tr>
<td>2</td>
<td>(?js%mwP</td>
</tr>
<tr>
<td>3</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td></td>
</tr>
</tbody>
</table>
Hello World

Clients 2 - n

Last known ID = 1

<table>
<thead>
<tr>
<th>ID</th>
<th>Encrypted</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Ba(3$rvj</td>
</tr>
<tr>
<td>2</td>
<td>(?js%mwP</td>
</tr>
<tr>
<td>3</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td></td>
</tr>
</tbody>
</table>
Solution
Secure RTCE-System

Client 1
Hello World!

Clients 2 - n

2. Enc(Op(add, !, 11), K_S)

<table>
<thead>
<tr>
<th>ID</th>
<th>Encrypted</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Ba(3$rvj</td>
</tr>
<tr>
<td>2</td>
<td>(?js%mwP</td>
</tr>
<tr>
<td>3</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td></td>
</tr>
</tbody>
</table>
Solution
Secure RTCE-System

Hello World
Dec(Enc(Op(add,1,11),K_S), K_S)

Clients 2 - n

<table>
<thead>
<tr>
<th>ID</th>
<th>Encrypted</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Ba(3$rvj</td>
</tr>
<tr>
<td>2</td>
<td>(?js%mwP</td>
</tr>
<tr>
<td>3</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td></td>
</tr>
</tbody>
</table>

Client 1
Hello World!

RTCE-Server
Solution
Secure RTCE-System

Client 1

RTCE-Server

ID | Encrypted
---|----------
1  | Ba(3$rvj
2  | (?js%mwP
3  | 
4  | 
5  | 

Hello World!
How to get the required $K_S$?

- A priori known by all clients
- Using a trusted key exchange server
- Using a hybrid encryption scheme
Transaction management

- No central document instance $\leftrightarrow$ Ensuring equal documents on each client
- Document modification requires knowledge about **all** previous modifications
- Storing document $\rightarrow$ cleanup of operations list
- How to handle inactivity?
• Defined Worfkflows to ensure equal document states on each client after short delay

• Implemented a prototype for encrypted RTCE based on the presented architecture and the workflows

• Verified the technical functionality
Open Tasks

• Up to now no existing identity management

→ Anyone may store operations on the RTCE-Server
→ System is vulnerable against adding useless operations

• Validating User-Acceptance

→ Do user want to secure their RTCE?
→ Do they accept the additional key management?
→ How to avoid additional effort?

• Benchmarking the system and proof its working correctly

• Implement plugins for existing open source projects
Thank you!
Any Questions?

Dipl.-Inf. Kevin Körner

kevin.koerner@uni-tuebingen.de
Phone: +49 7071 29-70384

Wilhelmstraße 106
72074 Tübingen
Germany