

Security in Distributed Systems

Christian Grothoff

Security in Distributed Systems

1. Build a DHT

- Build a simple discovery service where peers register their address and in return receive a random peer's address.
- Implement a protocol to populate routing tables of participants (suggestion: start with a clique).
- Add functions to PUT data into the DHT and to GET it back.
- Simulate churn and implement routing table maintenance.
- Analyze your design for security and performance.

Suggestion: for communication use either a REST API or UDP.

2. Partially offline payments

- Set up a Taler merchant backend and/or use the public one at <https://backend.demo.taler.net/> (user and password are “sandbox”).
- Withdraw some KUDOS to your Taler wallet so you could pay at the merchant backend.
- Install an OTP app on your phone.
- Configure an OTP device in the merchant backend and share the secret with your OTP app. Do **not** use the “with amount” mode, as canonical OTP apps do not support it!
- Create a template in the merchant backend and set up the OTP device for payment configuration.
- Scan the QR code of the template to initiate a payment.
- Pay and check the confirmation code from the payment configuration with your OTP app.