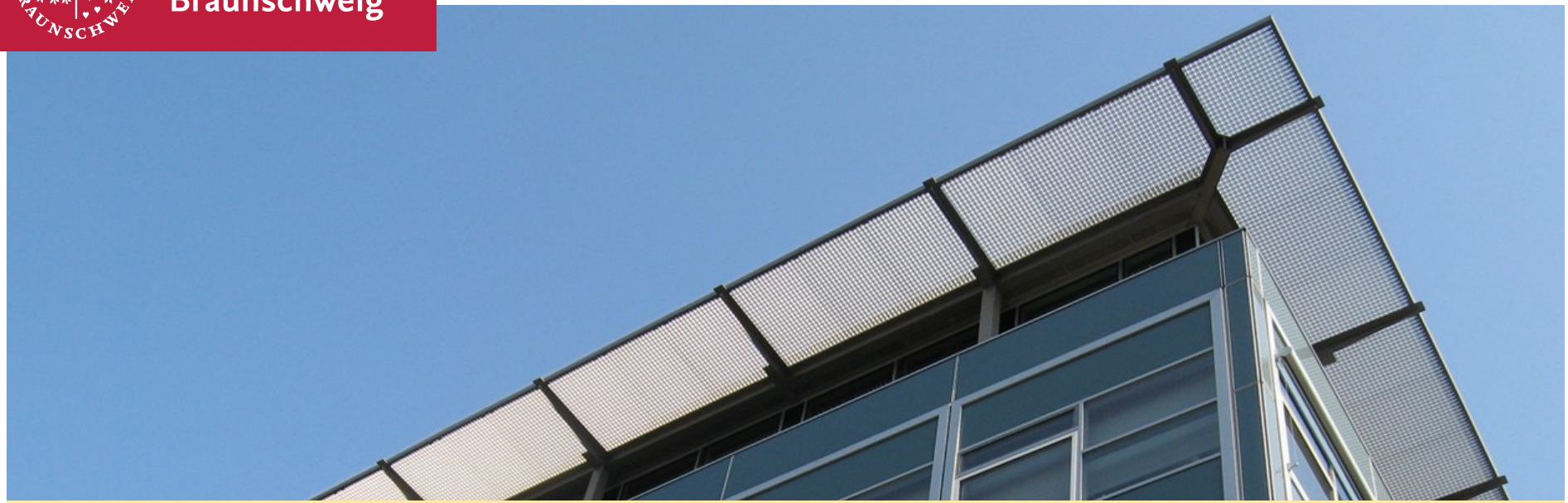
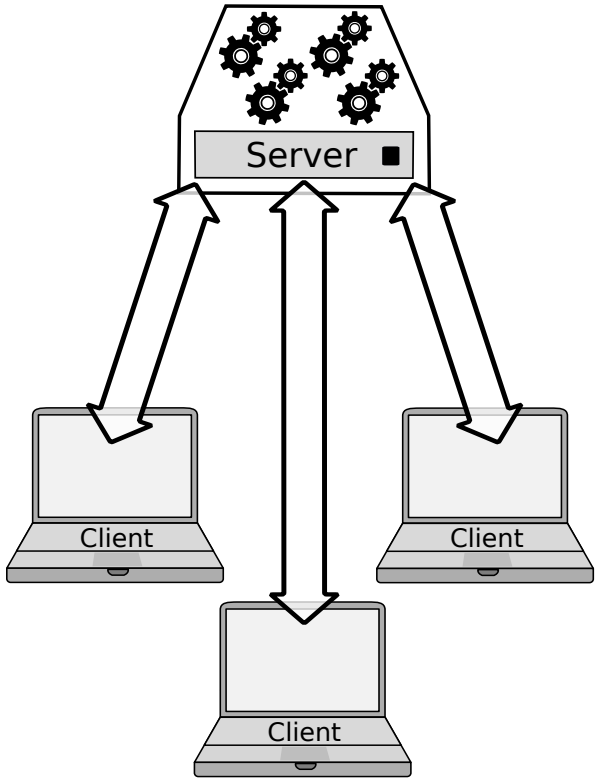


Practical Applications of Client-Side Trusted Computing

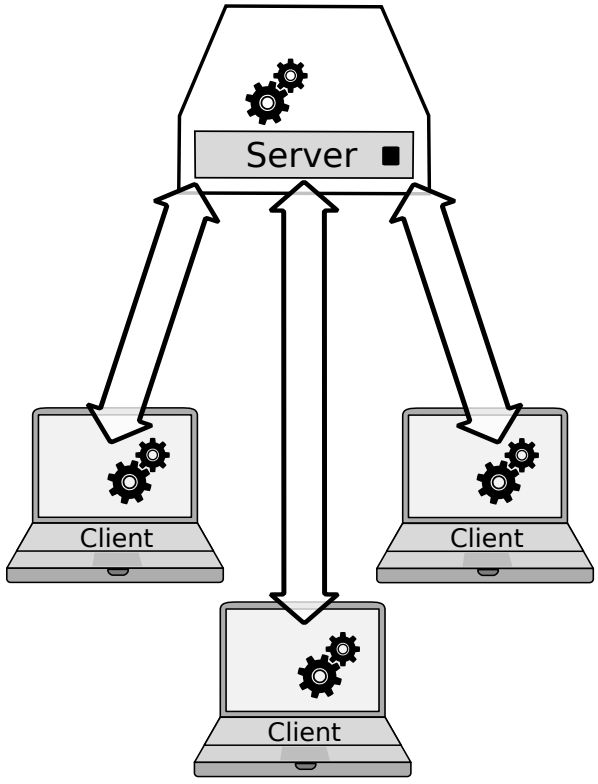
David Goltzsche, 2018-04-23

3rd year PhD student at distributed systems group, TU Braunschweig, Germany
Research area: trusted execution, distributed systems
Advisor: Rüdiger Kapitza

Overview

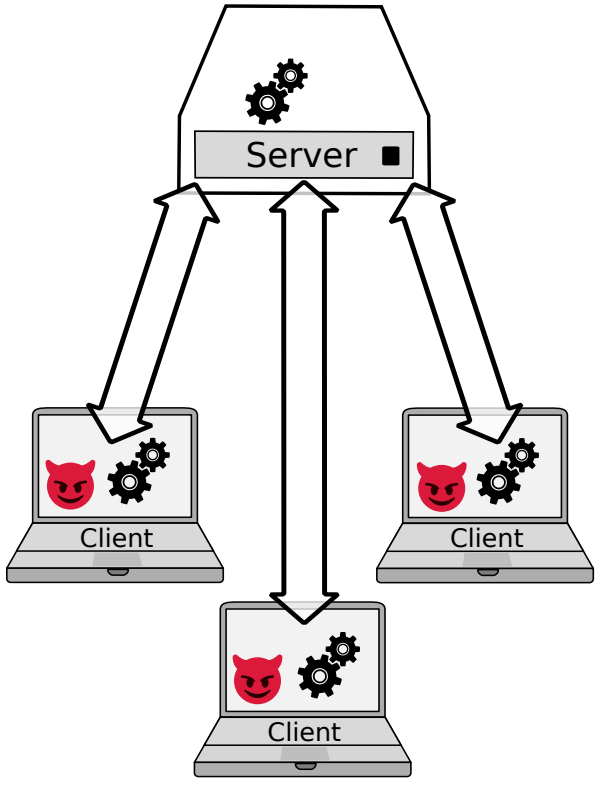


Overview



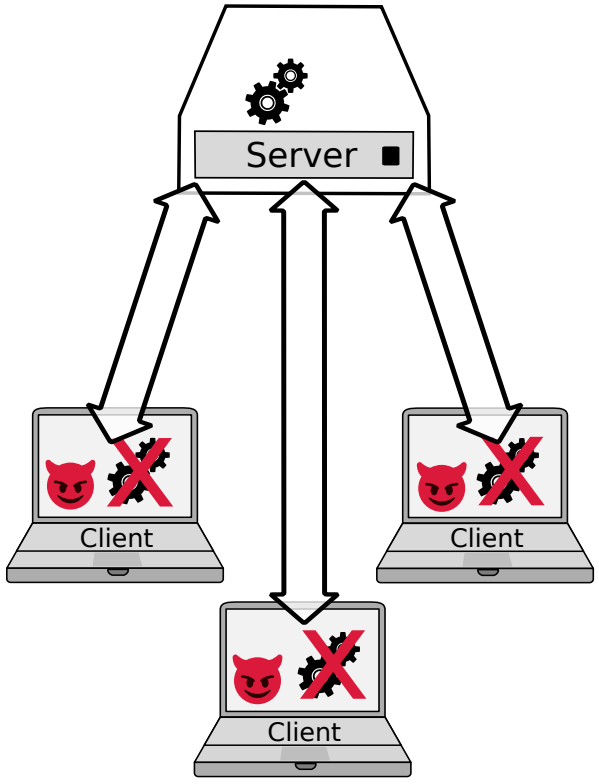
Overview

- **Problem:** offloading computations to **untrusted** clients is **limited**



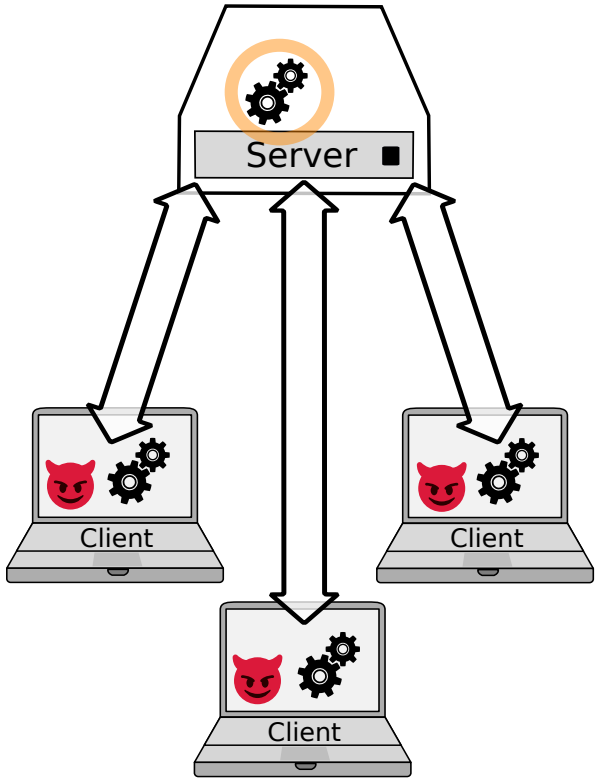
Overview

- **Problem:** offloading computations to **untrusted** clients is **limited**
- **Current best practice:** avoidance of offloading or expensive recomputations



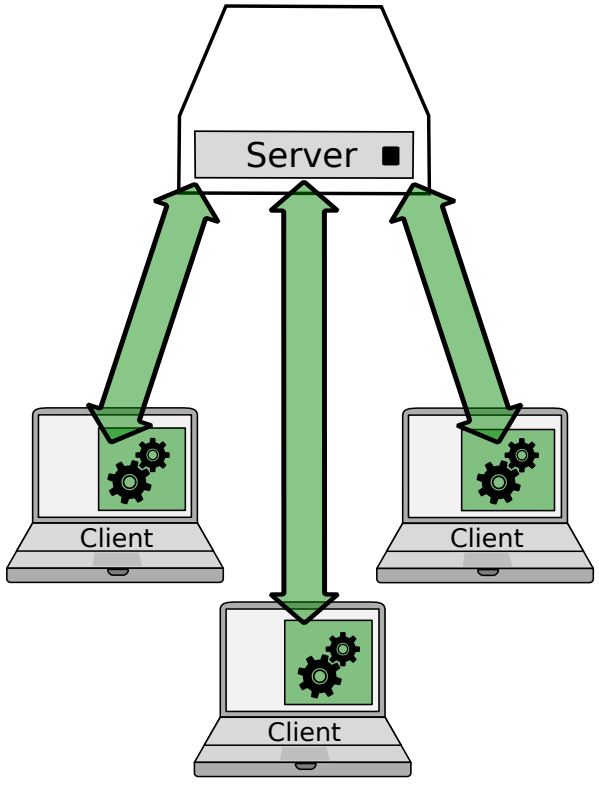
Overview

- **Problem:** offloading computations to **untrusted** clients is **limited**
- **Current best practice:** avoidance of offloading or expensive recomputations



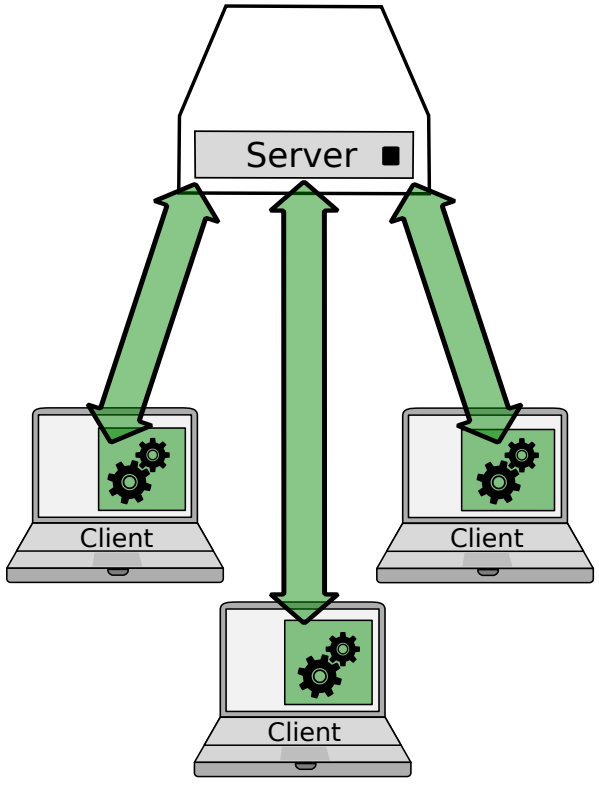
Overview

- **Problem:** offloading computations to **untrusted** clients is **limited**
- **Current best practice:** avoidance of offloading or expensive recomputations
- **Goal:** enable secure offloading using **client-side trusted computing**



Overview

- **Problem:** offloading computations to **untrusted** clients is **limited**
- **Current best practice:** avoidance of offloading or expensive recomputations
- **Goal:** enable secure offloading using **client-side trusted computing**
- **Consequence:** New paradigm for system design, because changed assumptions
  - How can existing systems be **redesigned**?
  - Which entirely **new use cases** are possible?

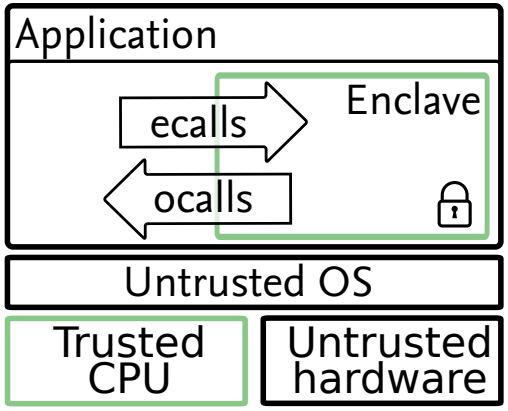


Trusted Execution Environments

- How to make **clients trusted**?

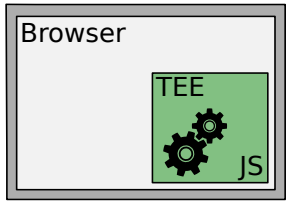
- Trusted Execution Environments (TEEs)
  - Data and execution protection
  - Memory encryption
  - Remote attestation

- Implementations
  - **Intel SGX**: available on commodity hardware
  - **Other vendors** expected to follow
  - Research: **Komodo** [Ferraiuolo et al., SOSP'17]



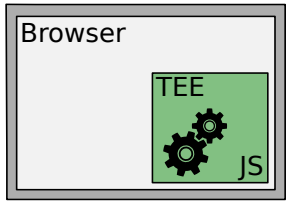
Use Cases of Client-Side TEEs

- JavaScript in Web Browsers **@EuroSec'17**
  - **Problem:** Recomputation in back-end of web application
  - **Solution TrustJS:** trusted client-side execution of JS

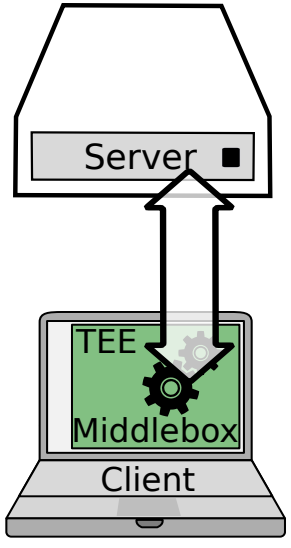


Use Cases of Client-Side TEEs

- JavaScript in Web Browsers **@EuroSec'17**
  - **Problem:** Recomputation in back-end of web application
  - **Solution TrustJS:** trusted client-side execution of JS

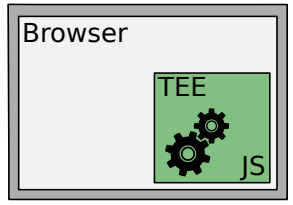


- Network Middleboxes **@DSN'18**
  - **Problem:** Client-side offloading **not considered** so far
  - **Solution EndBox:** client-side middlebox functions

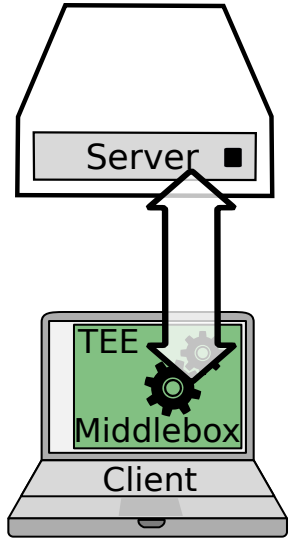


Use Cases of Client-Side TEEs

- JavaScript in Web Browsers **@EuroSec'17**
  - **Problem:** Recomputation in back-end of web application
  - **Solution TrustJS:** trusted client-side execution of JS



- Network Middleboxes **@DSN'18**
  - **Problem:** Client-side offloading **not considered** so far
  - **Solution EndBox:** client-side middleblox functions



- Volunteer Computing Systems
  - **Problem:** Jobs replicated to other clients to stop cheaters
  - **Solution TruVC:** trusted volunteer computing