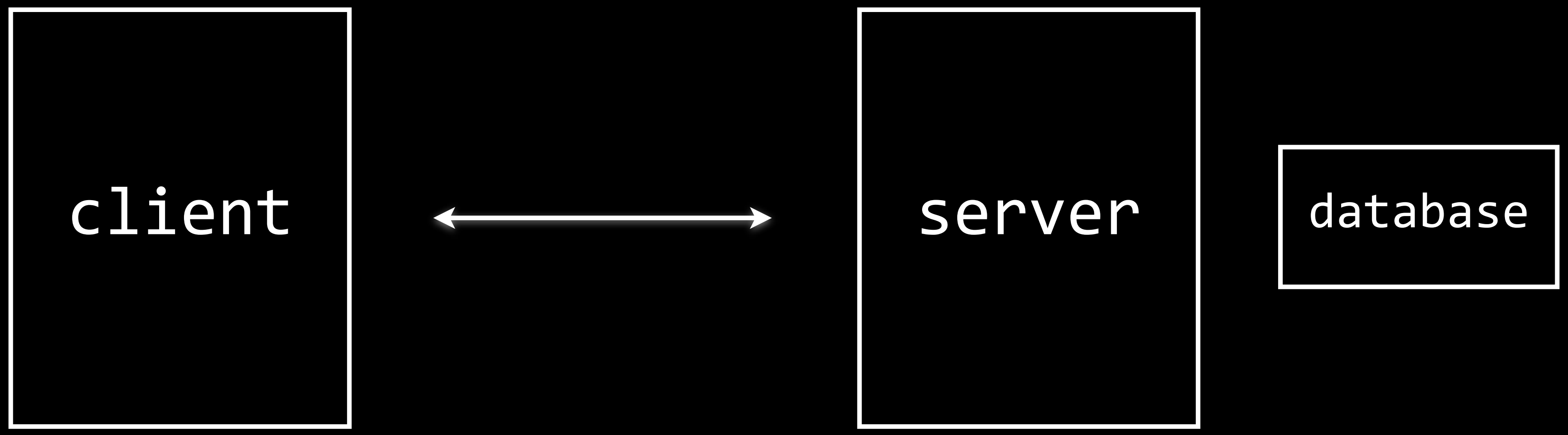
Security & Privacy

Last Man Standing

Parsia Hakimian
Kartik Thapar

Voting Machine System



`client`: user-end software

- Authentication Screen (`auth_screen`)
- Voting Ballot Screens (`group_screen`)

`server`:

- Handles requests from the client (authentication, approval)
- Database read/write functions
- Handles AuditLog & Result files

AuditLog & Result File

AuditLog —

```
{ hash(voterID + PIN) : {
    ‘president’ : [1]
    ‘congress’  : [2, 4]
    ‘counsel’   : [3]
    }
}
```

Result File —

```
{
    ‘president’ : [175, 100, 30]
    ‘congress’  : [20, 50, 140, 13, 164]
    ‘counsel’   : [44, 60, 25, 90]
}
```

Crypto

openSSL — to provide a secure connection

RSA — authenticate client, voter (server, etc.)

AES — (over SSL)

SHA — SHA256 to hash voterID and PIN; keep everything anonymous

Backdoor

There is a `backd00r`.