Click icon to add picture

Database Lab
Database Security

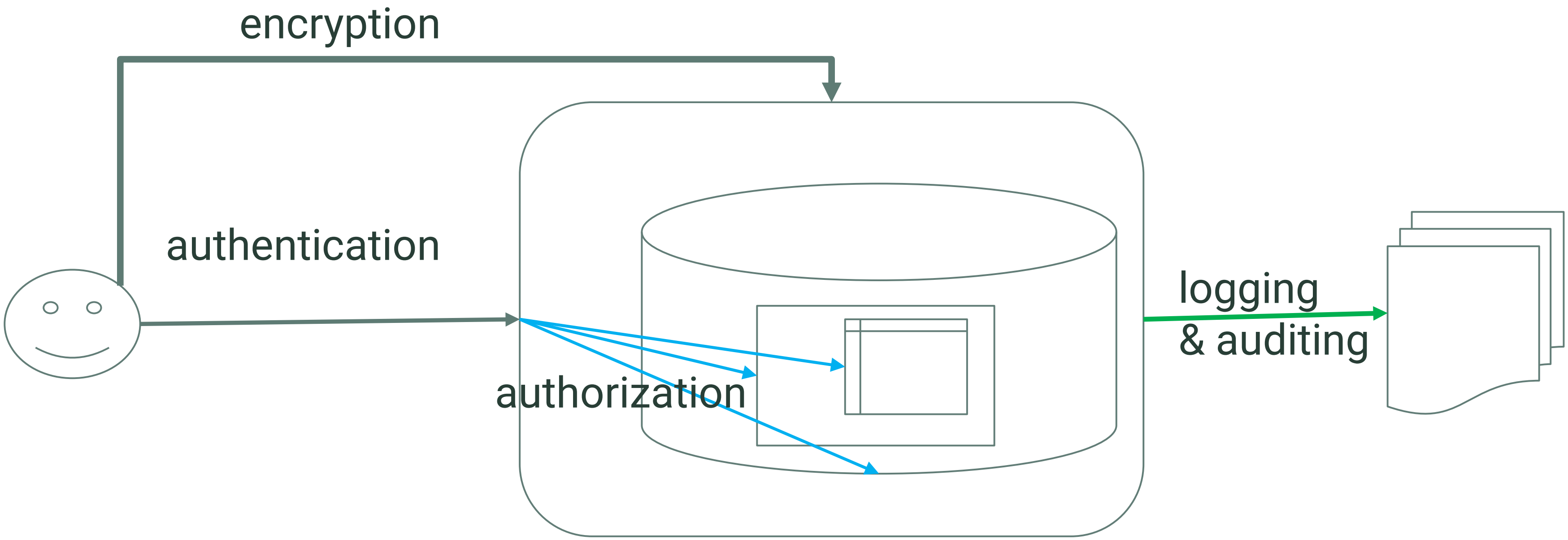
Fall Term 2023
Dr. Andreas Geppert
geppert@acm.org

Topics

- conceptual design
- logical design
- consistency constraints
- data manipulation
- queries
- transactions
- views
- stored procedures and user-defined functions
- triggers
- **security**

Database Security

- Authentication
- Authorization
- Auditing
- Encryption



Authentication

- Identification
- Proving that the claimed identity is the actual, real one
- In Postgres:
  - ~~trust~~
  - (operating system) identity
  - ~~password~~ (plain text)
  - hashed (~~MD5~~, SCRAM-SHA-256)
  - LDAP
  - many more …

Authentication
The pg_hba.conf file

- defines authentication and connectivity parameters

```
TYPE    DATABASE    USER    IP-ADDRESS    IP-MASK    METHOD    OPTIONS
local   all         postgres                         peer
local   all         cashu                            trust
host    cashdb      cashu   127.0.0.1/32             SCRAM-SHA-256
hostssl cashdb      cashu   10.22.0.0/16             SCRAM-SHA-256
host    all         all     0.0.0.0/0                reject
```

Authorization

- ensures that users/applications are actually permitted to perform the actions they would like to execute
- privilege: grants a permission to a user or role
  - grant and revoke statements
- important system privileges in Postgres
  - create user/role,
  - create database
  - create object privilege
- important object privileges
  - connect to database
  - schema usage
  - select, insert, update, delete, truncate table
  - execute function

Authorization

- roles represent functions and have the permissions required to perform these functions
  - create role statement
  - grant and revoke roles from other roles or users

- fine-grained access control
  - permissions not just on table-level, but data-dependent
  - e.g., bank users can only see their own accounts
  - possible in Postgres

Logging and Auditing

- Database servers protocols certain activities (logging)
- Debugging
- User support
- Traceability
  - who did what when
  - for instance, who dropped a certain table??
  - Auditing

Encryption

- Data-in-transit
  - Encrypts communication between server and clients/applications
  - Communication cannot be intercepted or modified
  - psql «host=127.0.0.1 dbname=cashdb **sslmode=verify-full**» -U cashu
- Data-at-rest
  - Sensitive/secret data are encrypted inside the database
  - Application encrypts data before storing and decrypts after reading
  - See extension pg_crypto