COMP 9322
Software Service Design and Engineering

Lecture 3 – Advanced API Topics

Disclaimer

- Some of the Slides are Taken from previous Years offerings

API Security

- Security is sometimes overlooked for the sake of rabid development and release and that causes security breaches.
- OWASP included many instances in their web security Top ten related to APIs and they have the REST Security cheat sheet.
- REST relies on the elements of the Web for security too (Check OWASP top 10)
- Things to remember (Input Validation, Methods restriction, logging)

https://www.owasp.org/images/7/72/OWASP_Top_10-2017_%28en%29.pdf.pdf
https://www.owasp.org/index.php/REST_Security_Cheat_Sheet

REST APIs and Security

HTTPS (SSL)

- "Strong" server authentication, confidentiality and integrity protection The only feasible way to secure against man-in-the-middle attacks
- Any security sensitive information in REST API should use SSL

See the OWASP Transport Layer Protection Cheat Sheet

https://www.owasp.org/index.php/Transport_Layer_Protection_Cheat_Sheet

REST APIs and Security (Cont'd)

API developers at least must deal with authentication and authorisation:

Authentication (401 Unauthorized) vs. Authorisation (403 Forbidden):

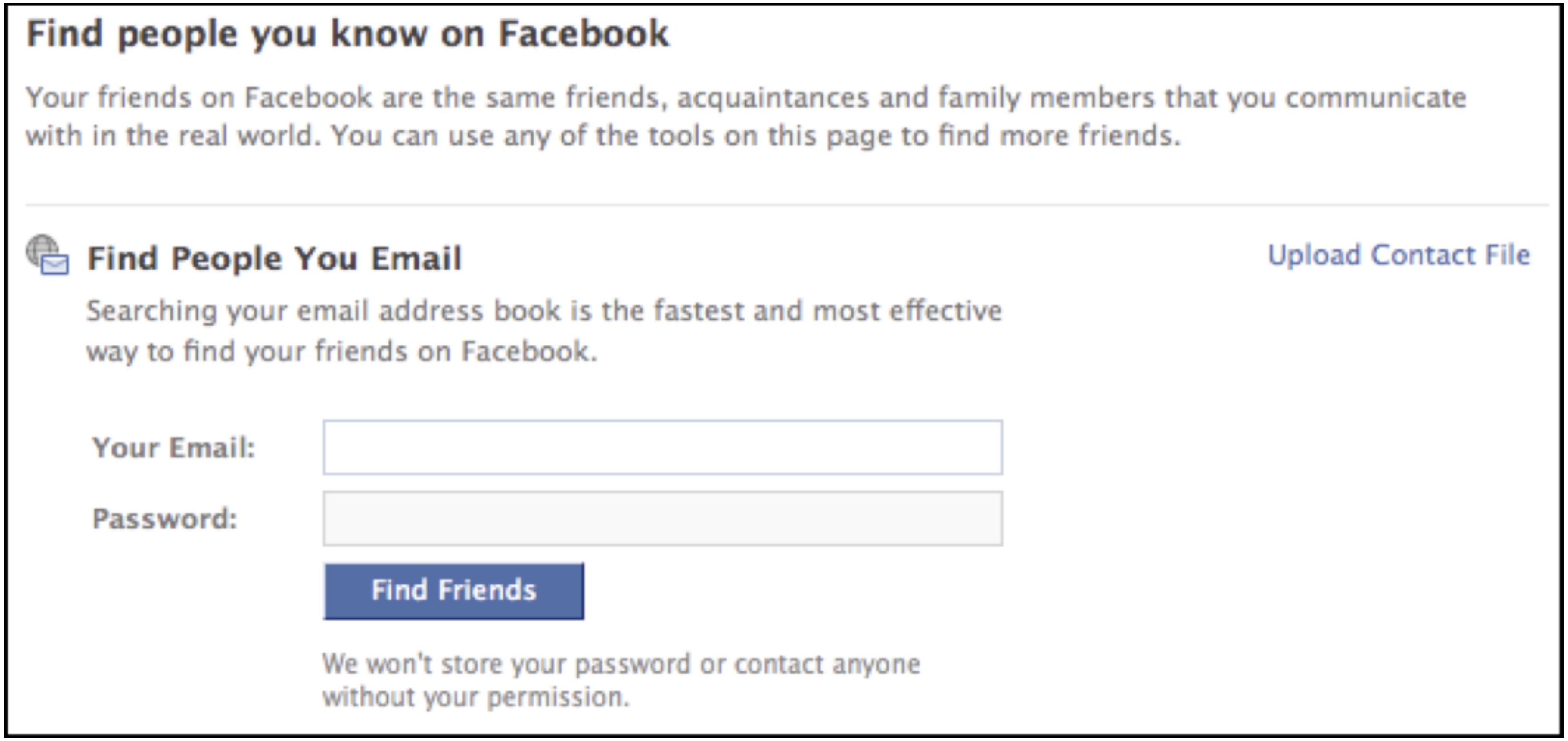
Common API authentication options:

- HTTP Basic (and Digest) Authentication: IETF RFC 2617
- Token-based Authentication (e.g., JWT)
- API Key [+ Signature]
- OAuth (Open Authorisation) Protocol - strictly uses HTTP protocol elements only

https://www.owasp.org/index.php/Transport_Layer_Protection_Cheat_Sheet

OAuth

- OAuth tries to solve this problem …



Find people you know on Facebook

Your friends on Facebook are the same friends, acquaintances and family members that you communicate with in the real world. You can use any of the tools on this page to find more friends.

Find People You Email

Upload Contact File

Searching your email address book is the fastest and most effective way to find your friends on Facebook.

Your Email:

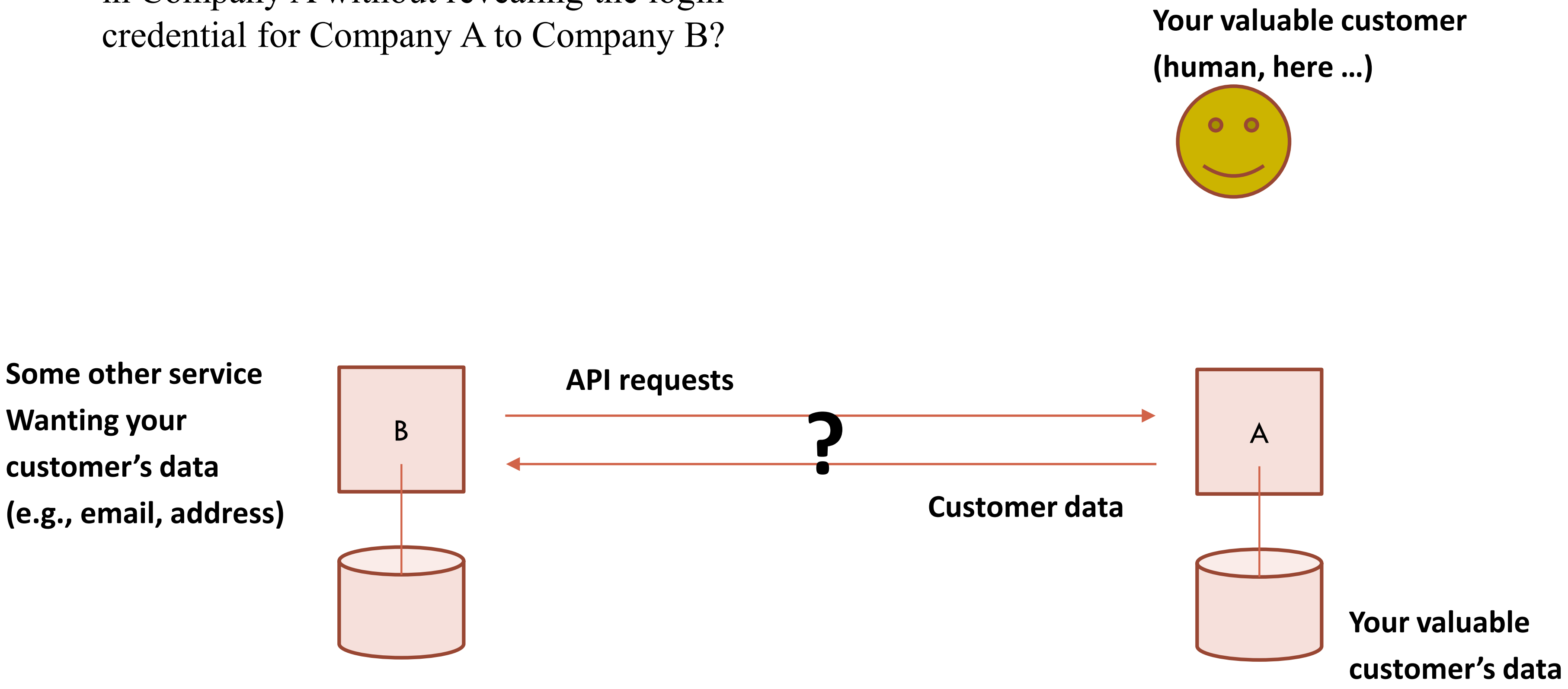
Password:

We won't store your password or contact anyone without your permission.

- Essentially, an authorisation scheme for data access …

OAuth (RFC-6749)

How does the user allow Company B to access the data in Company A without revealing the login credential for Company A to Company B?



Your valuable customer (human, here …)

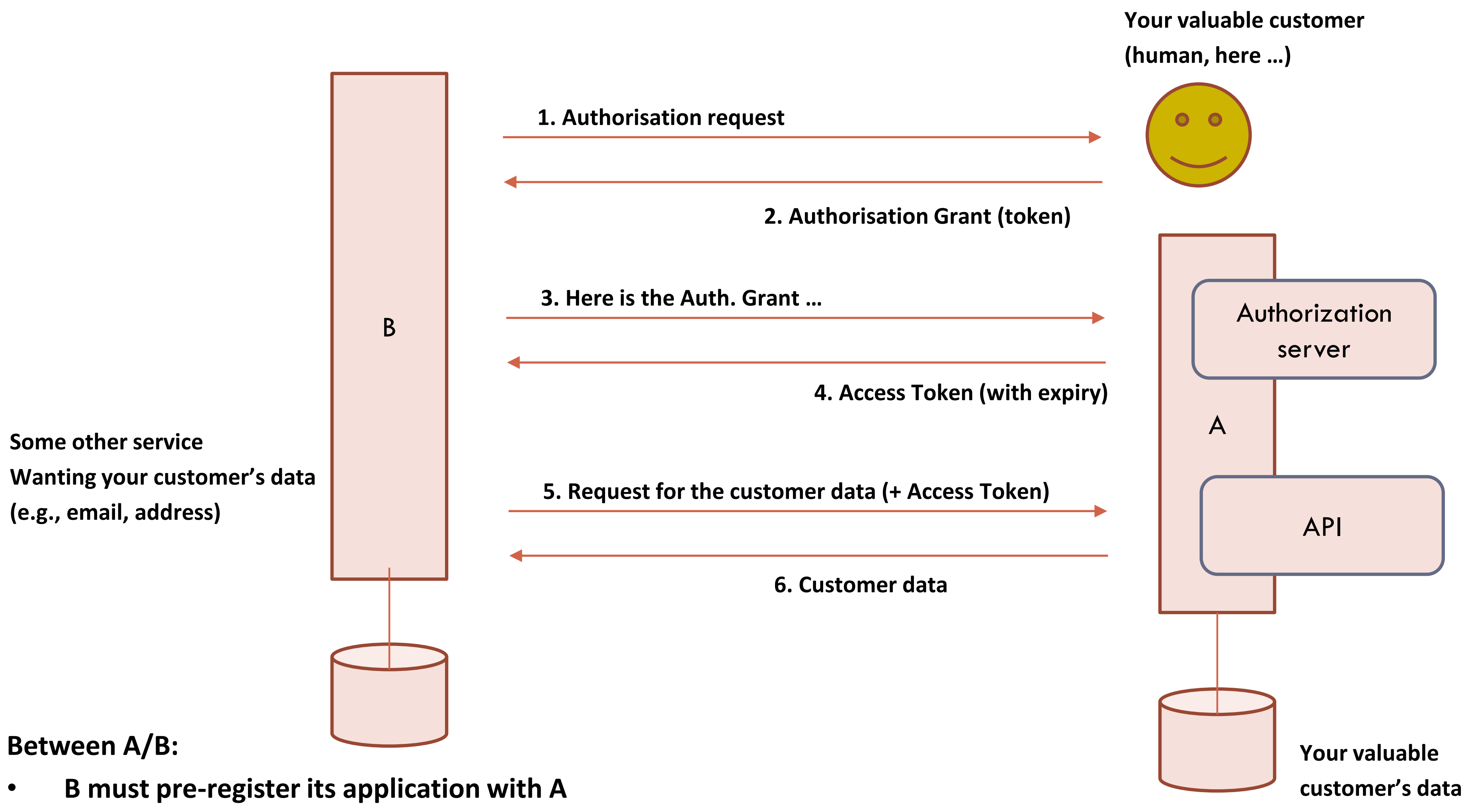
Some other service Wanting your customer’s data (e.g., email, address)

API requests

Customer data

Your valuable customer’s data

OAuth workflow (e.g., social login scheme)


Your valuable customer
(human, here …)
1. Authorisation request
2. Authorisation Grant (token)
3. Here is the Auth. Grant …
4. Access Token (with expiry)
5. Request for the customer data (+ Access Token)
6. Customer data
B
A
Authorization server
API
Some other service
Wanting your customer's data
(e.g., email, address)
Your valuable customer's data

Between A/B:

- B must pre-register its application with A
- A issues 'API key' and Secret for B (for Authentication of B)
- Authorisation to data (per customer) is done through OAuth

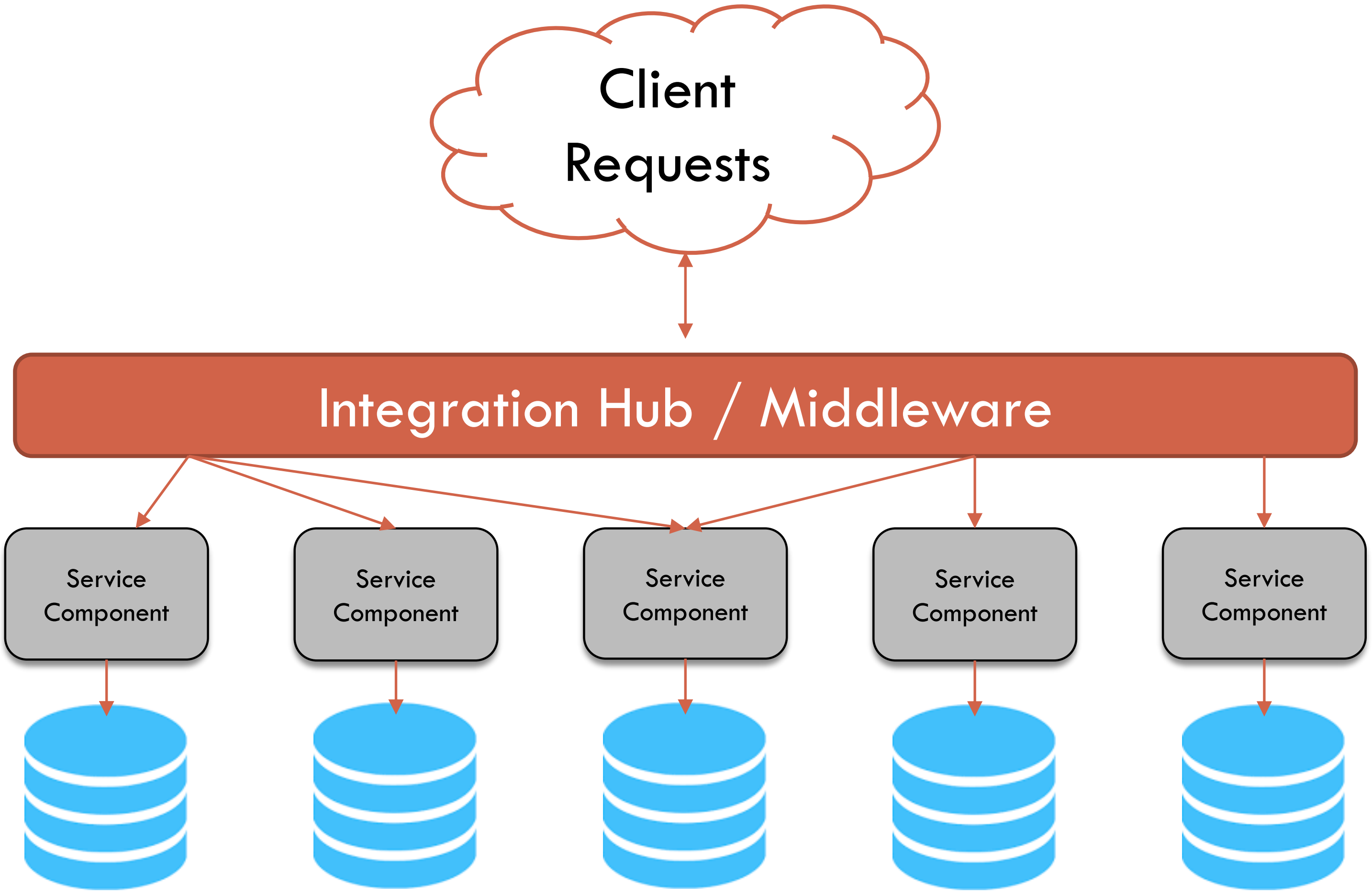
OAuth has different scope

Facebook:
https://developers.facebook.com/docs/facebook-login/access-tokens

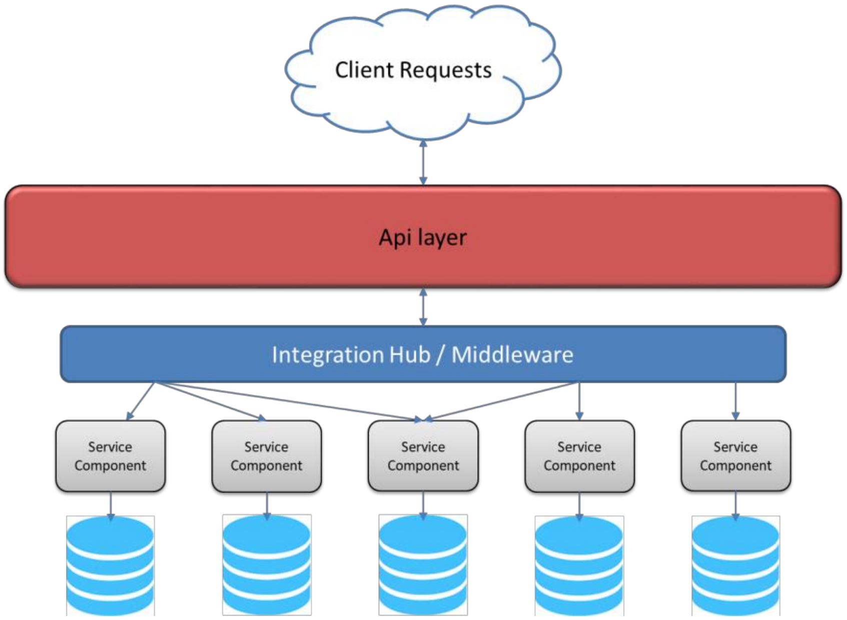
Spotify:
https://beta.developer.spotify.com/documentation/general/guides/scopes/

Should consider the scope during the design of OAuth scheme for your API.

Integration Hub (API Gateway)

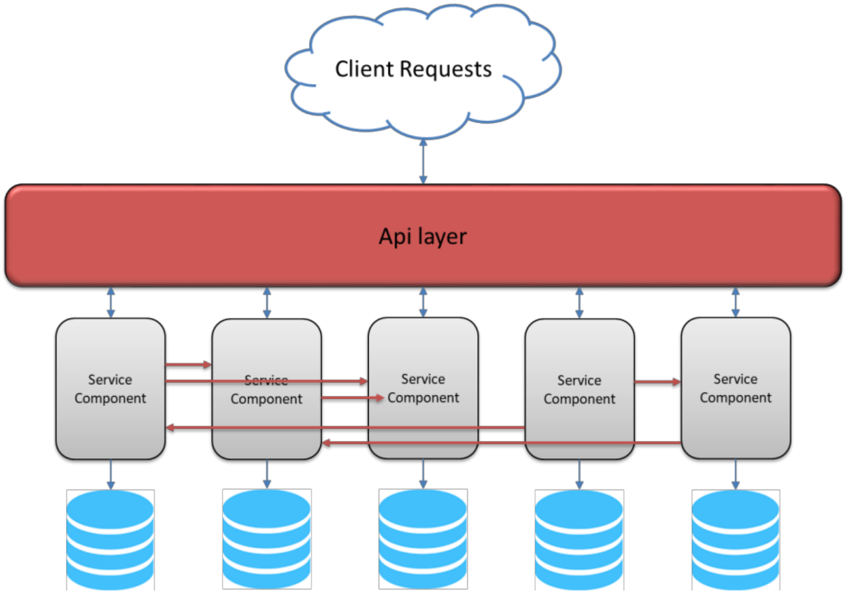


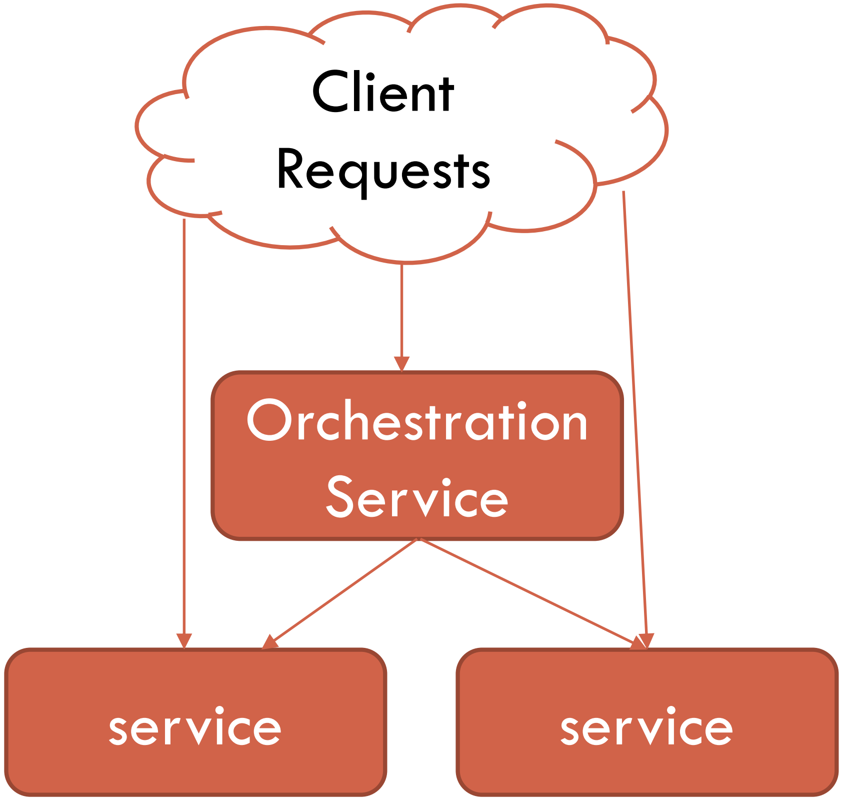
Why Use API Gateway



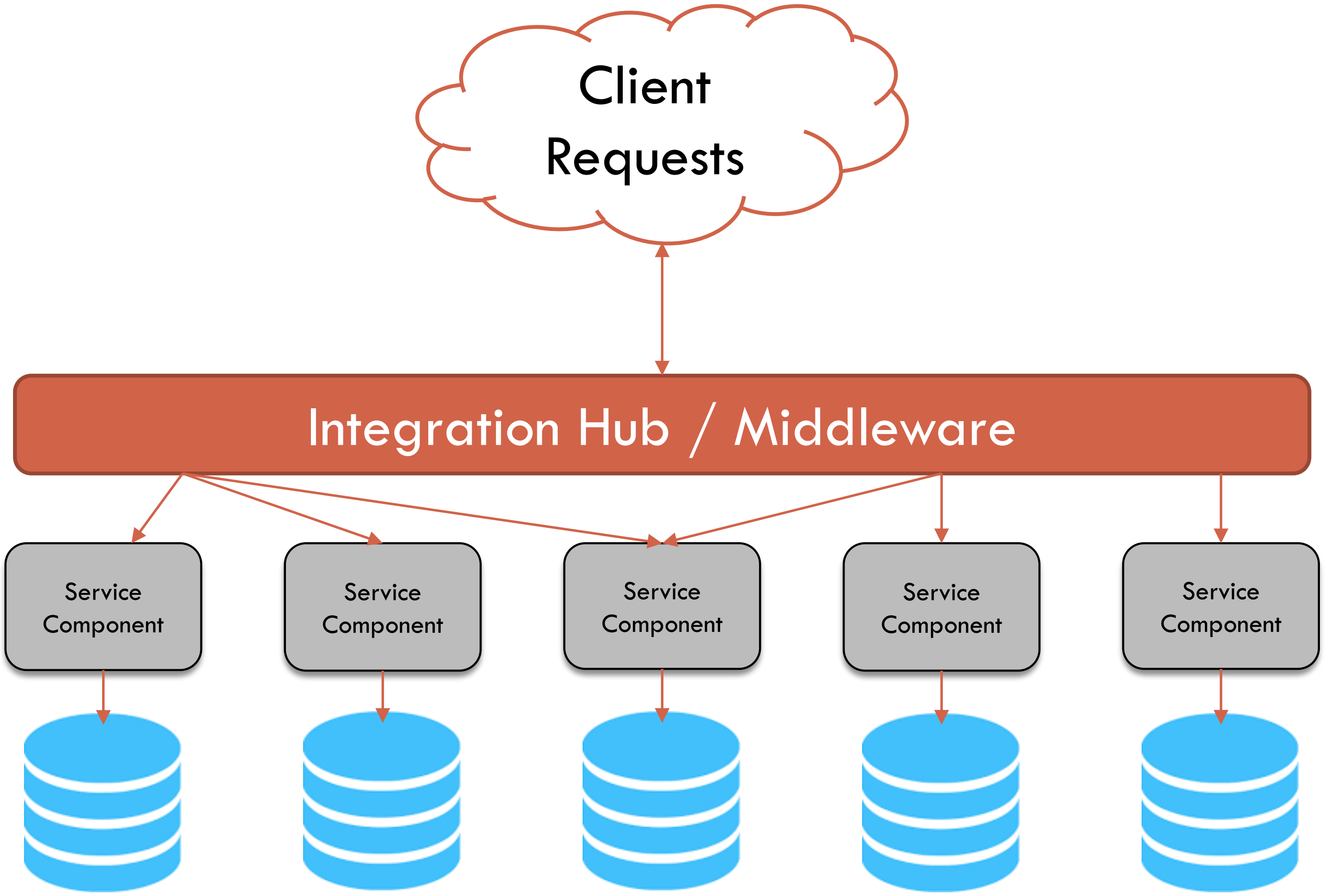
- Service Orchestration
- Protocol Transformation

Service Orchestration

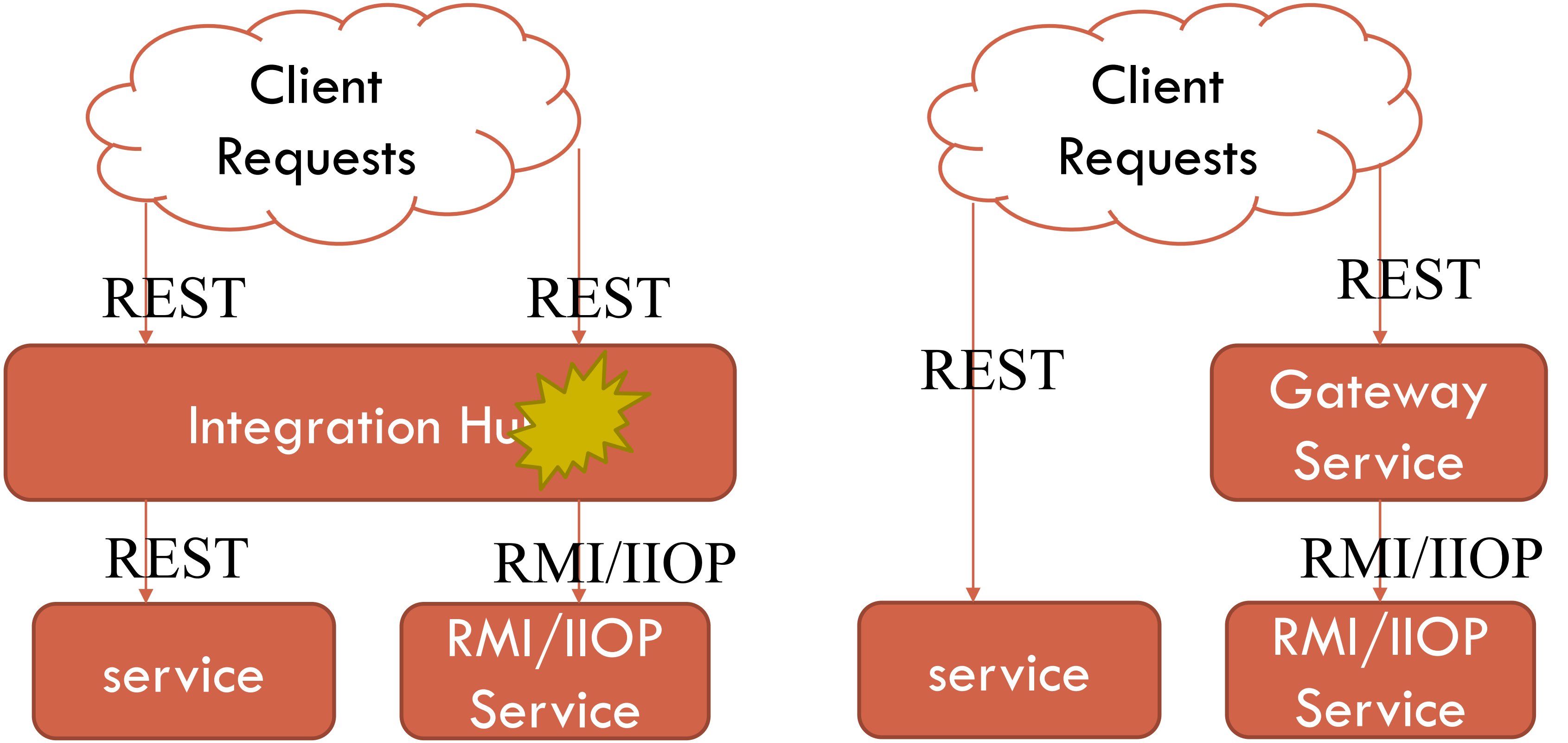




Service Orchestration



Protocol Transformation



Some API Gateways out there

- Example:
  - Netflix API Gateway
- Solutions:
  - Amazon API Gateway
  - Kong
  - Mulesoft
  - Apigee

https://medium.com/netflix-techblog/optimizing-the-netflix-api-5c9ac715cf19

Questions?