RIPE

HTTP State Management Mechanisms with Multiple Addresses User Agents

draft-vyncke-v6ops-happy-eyeballs-cookie-01

RIPE 70, May 2015, Amsterdam, NL
IPv6 WG

Eric Vyncke evyncke@cisco.com @evyncke

RIPE

HTTP Session Cookie

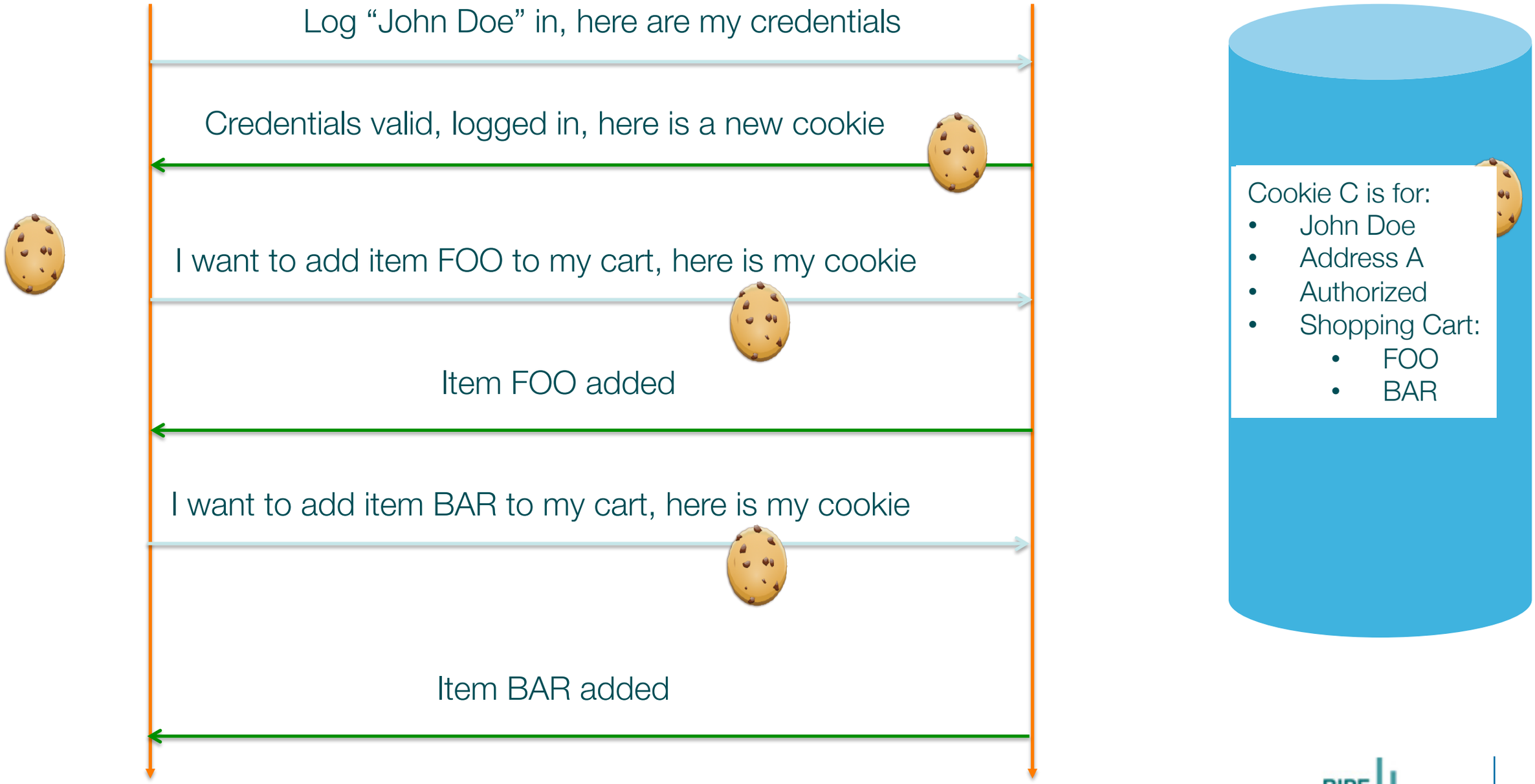
Source: wikimedia and Pinheiro

- HTTP has no transaction concept
- Application stores transaction states (e-commerce cart) on the server as a ‘session’
- ‘sessions’ are identified by an opaque value which is unique for the length of the transaction
  - This value is transported as a HTTP header cookie
  - This value is usually an index into a server table containing all transactions
- To prevent ‘session hijacking’, some servers store the client IP address and check it on each HTTP request

Session Cookies at Work

John Doe with IP address A

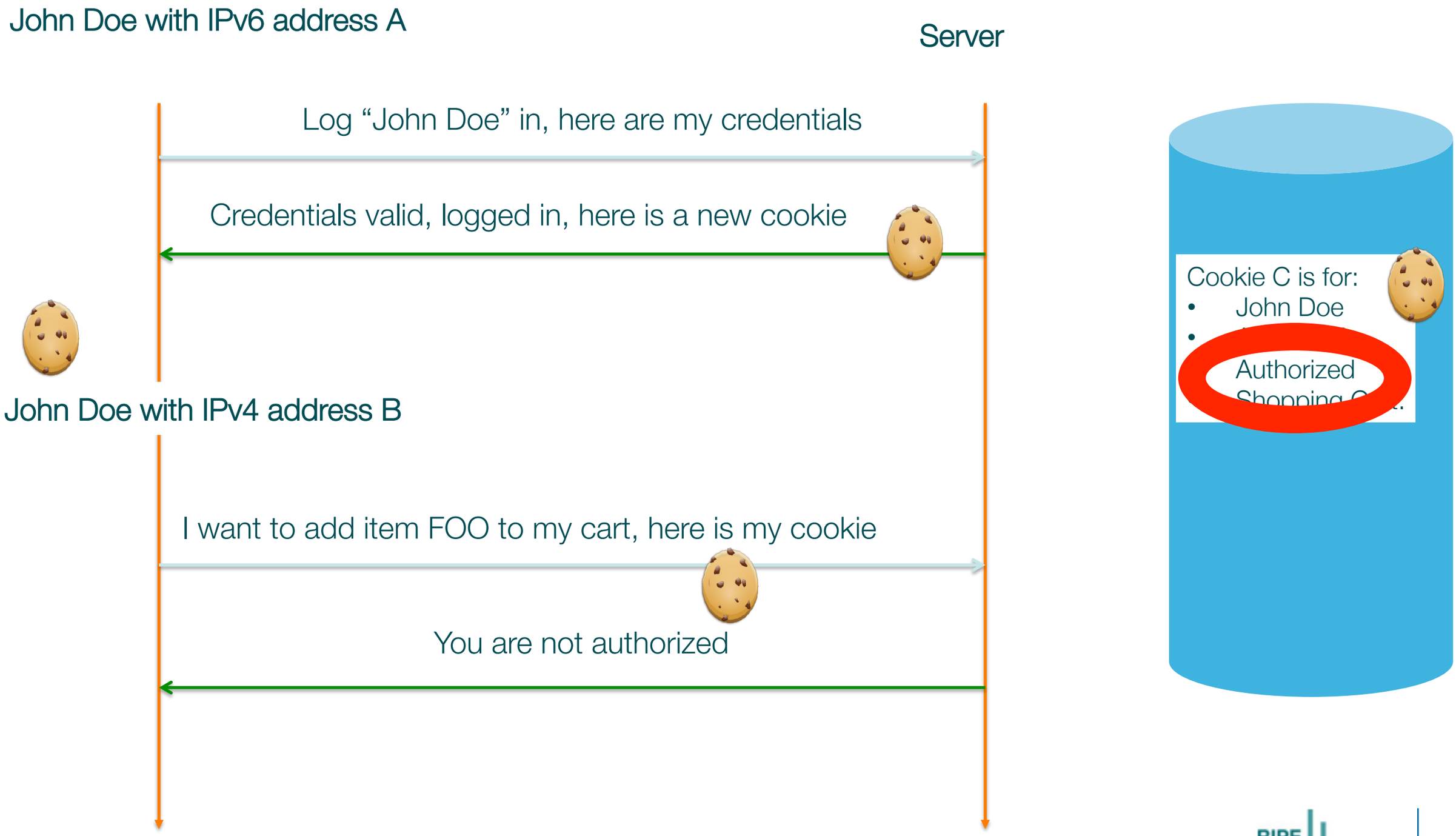
Server



Session Cookie and IP Address Change

- User starts a transaction with IP address A
- Server allocates cookie C
- Server stores address A and checks it for all HTTP requests having cookie C
- The CRUX:
  - Happy Eyeball (RFC 6555) switches address family and use address B
  - CGN change address to B (non RFC 6888 compliant)
- Next requests from user still uses cookie C but comes from address B
- Server checks the address, A != B and server refuses the request

Session Cookies Changing Address



Symptom of HTTP Requests being Denied

- Return to login screen
- or

Impact of IPv6 Deployment

- At least two content providers in Belgium have stopped dual-stack deployment
  - Infosec not ready to unlink session cookie from IP address
- It is slowing down IPv6 content deployment

Summary

- One IP address does not mean one user anymore
- Changing of IP address on the course of a session causes problems

- RFC 6883 section 8.2 briefly mention this
- Caused by CGN, Happy Eyeball, Multi-Interface,...
- MPTCP should solve it (if widely implemented)
- Working with OWASP to fix:
  - https://www.owasp.org/index.php/Session_Management_Cheat_Sheet

Questions?