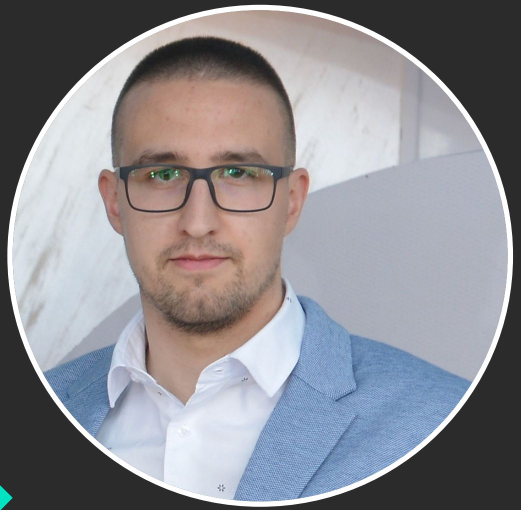
droidcon academy

Authentication in Ktor



Stefan Jovanović

𝕏 @StevdzaS

in in/stevdza-san

Overview

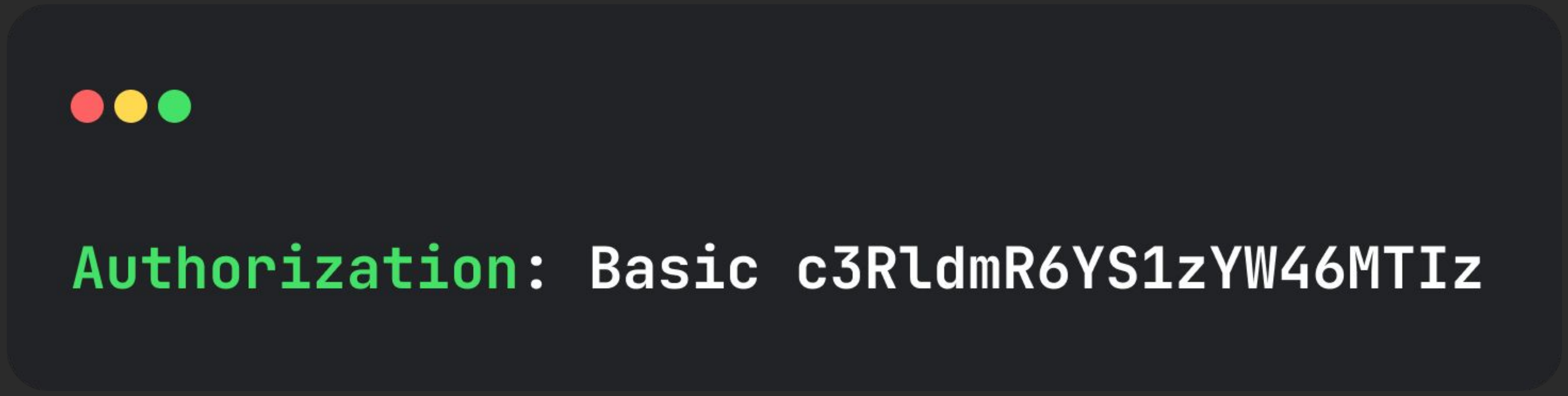
- Authentication Schemes
- Bearer Authentication
- Summary

Authentication Schemes

- Basic
- Digest
- Bearer

Basic Authentication

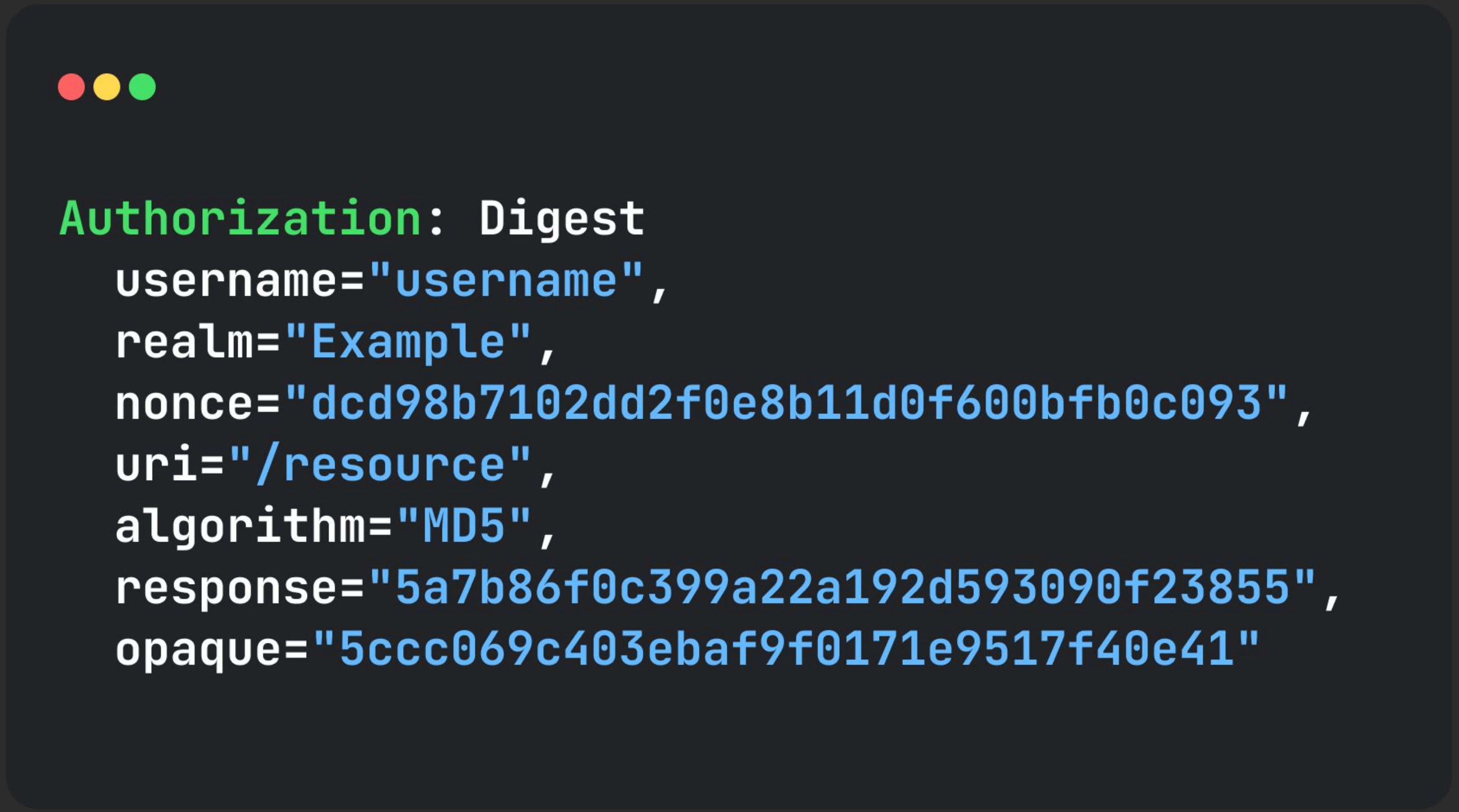
- User credentials in each request
- Base-64 encoded
- username:password
- Encoded, not encrypted
- HTTPS required



```
Authorization: Basic c3RldmR6YS1zYW46MTIz
```

Digest Authentication

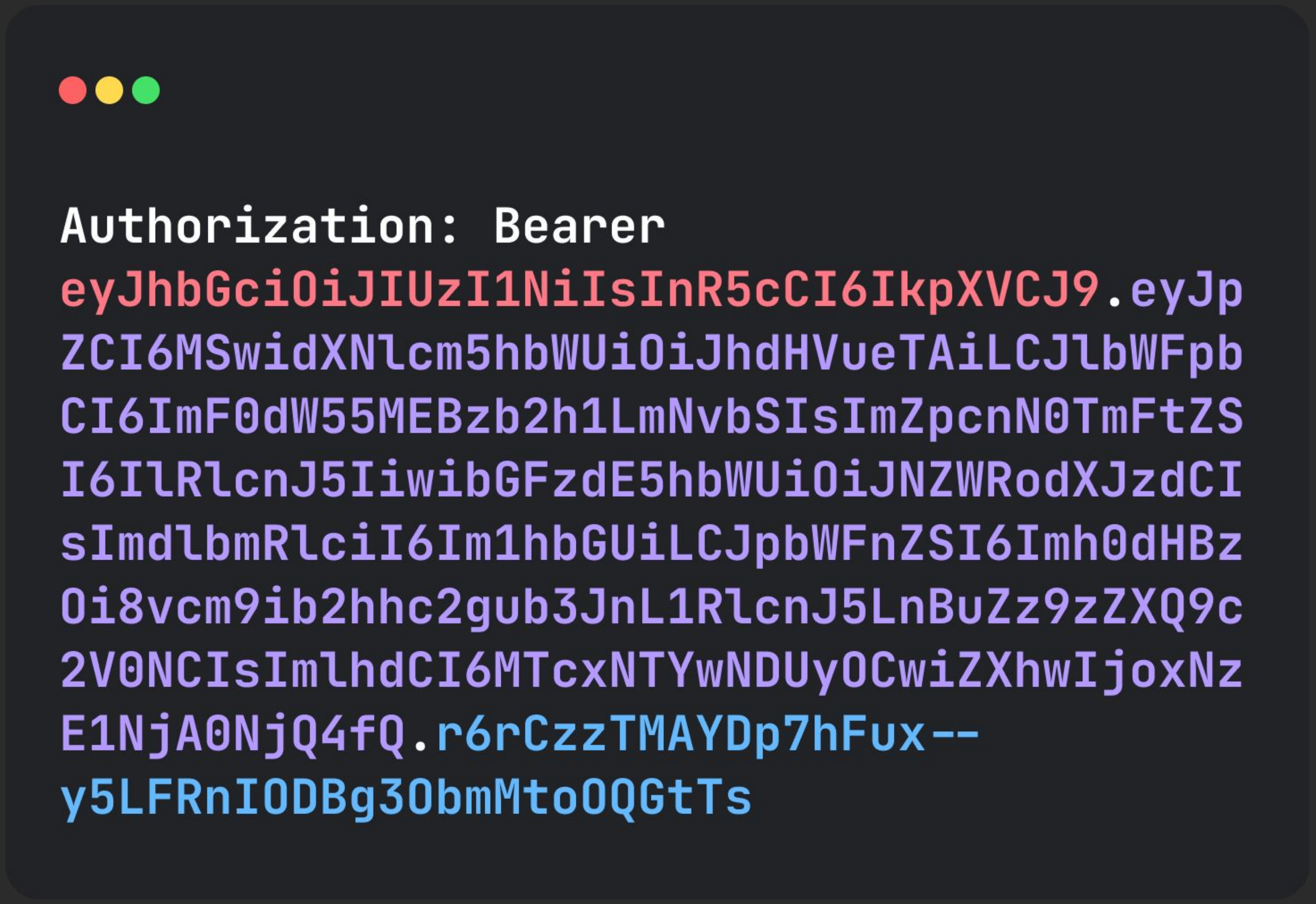
- Password is NOT sent in clear-text
- Server responds with a challenge
- Nonce (Unique value)
- Realm (Protected resource)
- Client creates a hash
- Server verifies it
- Vulnerability to replay attacks



```
Authorization: Digest
  username="username",
  realm="Example",
  nonce="dcd98b7102dd2f0e8b11d0f600bfb0c093",
  uri="/resource",
  algorithm="MD5",
  response="5a7b86f0c399a22a192d593090f23855",
  opaque="5ccc069c403ebaf9f0171e9517f40e41"
```

Bearer Authentication

- Used by modern applications
- Server generates a Token
- Client includes Token with each request
- Server verifies the signature/expiration
- Used along with HTTPS (Secure protocol)



```
Authorization: Bearer
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJp
ZCI6MSwidXNlcm5hbWUiOiJhdHVueTAiLCJlbWFpb
CI6ImF0dW55MEBzb2h1LmNvbSIsImZpcnN0TmFtZS
I6IlRlcnJ5IiwibGFzdE5hbWUiOiJNZWRodXJzdCI
sImdlbmRlciI6Im1hbGUiLCJpbWFnZSI6Imh0dHBz
Oi8vcm9ib2hhc2gub3JnL1RlcnJ5LnBuZz9zZXQ9c
2V0NCIsImlhdCI6MTcxNTYwNDUyOCwiZXhwIjoxNz
E1NjA0NjQ4fQ.r6rCzzTMAYDp7hFux--
y5LFRnIODBg3ObmMtoOQGtTs
```

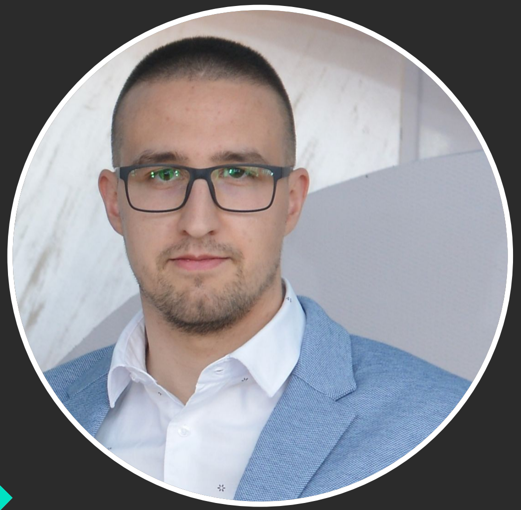
Bearer Authentication

- JWT (JSON Web Token)
- Secure transmission
- OAuth provider (Google, Facebook)
- 30-60 minutes
- Include token with each request
- Token refresh

Summary

- Various authentication schemes
- Bearer authentication and tokens
- Refresh tokens
- Network Inspector

Thank you!



Stefan Jovanović

𝕏 @StevdzaS

in in/stevdza-san