Securing Authentication, Sessions and Access Cont.

- **Sessions:** Managing user activities across application and devices
- Set of data structures tracking user's interaction with application server-side
- **Unique unforgeable secret** sent automatically after receipt back to server by client for identification
- May employ cryptography for enhanced security
- May be stored in Cookies or browser local storage

https://cheatsheetseries.owasp.org/cheatsheets/Session_Management_Cheat_Sheet.html

Securing Authentication, Sessions and Access Cont.

- **Access Control:** Fine-grained logic to determine R/W permissions per user or object.
- Determines if a user is authorized to perform an action
- Often implemented as roles
- Avoid assumptions as to how users might interact with the application

https://cheatsheetseries.owasp.org/cheatsheets/Session_Management_Cheat_Sheet.html