Seminar Conference 2019

Multi-Factor Authentication with Asynchronous Token and Short Message Service

Angel Anna Mathew,

MEng in Internetworking (angel.mathew@dal.ca)
1360 Barrington St. Halifax, NS. B3J 1Z1

DALHOUSIE UNIVERSITY
Inspiring Minds

MULTI-FACTOR AUTHENTICATION BY ASYNCHRONOUS TOKEN AND SMS

NEED OF MFA

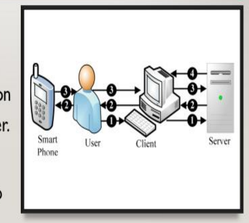
- REDUCE SECURITY BREACH
- INCREASE LEVELS OF SECURITY
- COMBINES AUTHENTICATION BY KNOWLEDGE AND OWNERSHIP

HOW MFA IS ACHIEVED

- Identification with user credentials
- SMS with challenge question to user's mobile phone, using Twilio helper library
- Mobile application as the asynchronous token to generate response key

MFA FRAMEWORK

- Identification with user credentials.
- SMS with challenge question to user's registered number.
- Mobile application acts as the asynchronous token to generate response key



MFA TECHNOLOGIES

- Authentication by time factor-based challenge
- Authentication by ownership
- Authentication by knowledge

IDENTIFICATION WITH USER CREDENTIALS

Users with valid credentials alone, passes the first step of authentication.

Credentials are :

User-name | Password

LOGIN PAGE AND SMS RECEIVED ON USER MOBILE

- SMS contains time factor-based challenge question

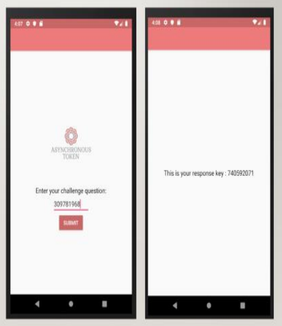
CHALLENGE QUESTION

Challenge question generation :

- Encrypt the combination of time factor and random number
- Key of encryption – base64 encoded value of user pin
- Hash the value of encrypted combination

ASYNCHRONOUS SOFT TOKEN

- Input : Challenge question
- Output : Response key



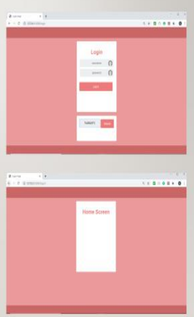
RESPONSE KEY

Hashed value of the challenge question

hashCode() method in Java is used to generate the value

HOME PAGE

- User enters the response key
- User is taken to home page



CONCLUSION

- Authentication by possession
- Authentication by ownership
- Out of band method to send SMS provides separate communication channel
- Increased levels of security