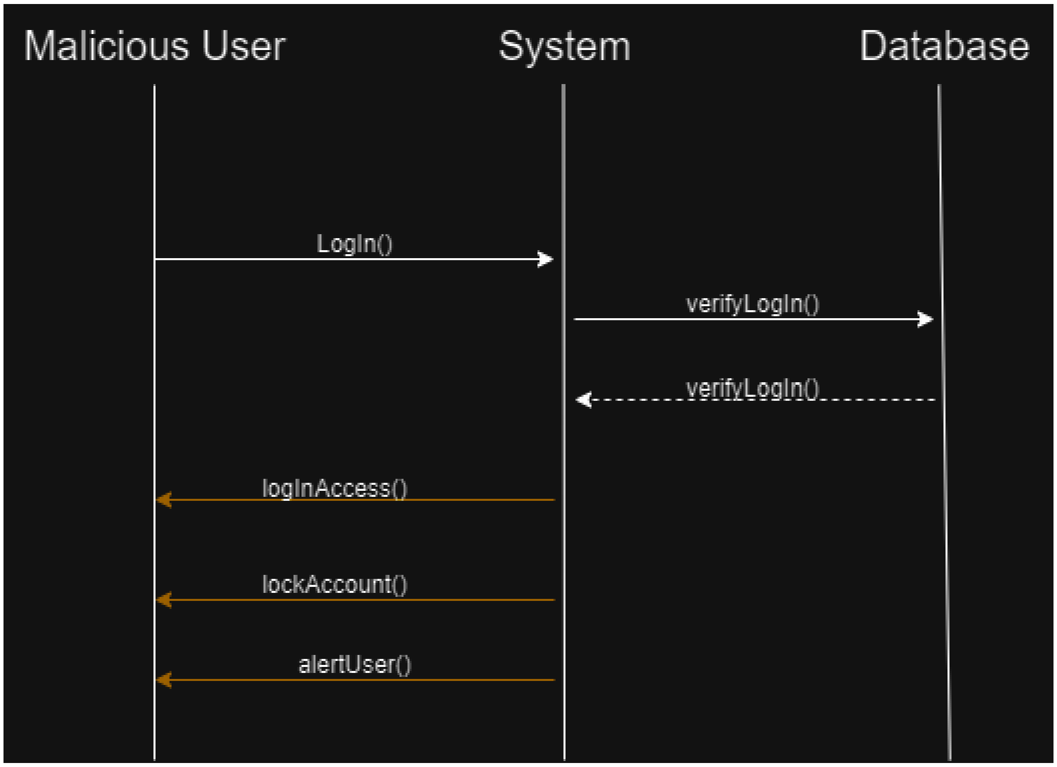
Abuse Use Case - Brute Force/Dictionary Attack

A Malicious Actor uses brute force algorithms or online password dictionaries in an attempt to forcefully guess a user's password.

SSD



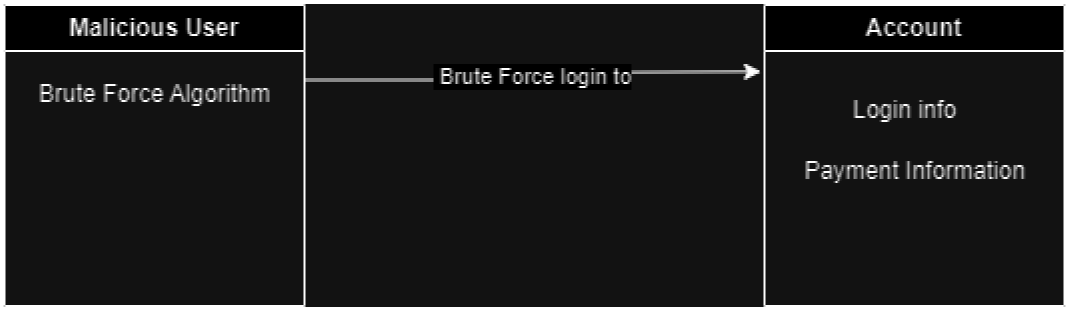
Operation Contracts

Operation	loginAccess()
Cross-Reference	Brute Force/Dictionary Attack
Precondition	User login info has been verified as either valid or invalid
Postcondition	User is granted or denied access to the account, if denied, the number of failed login attempts is incremented

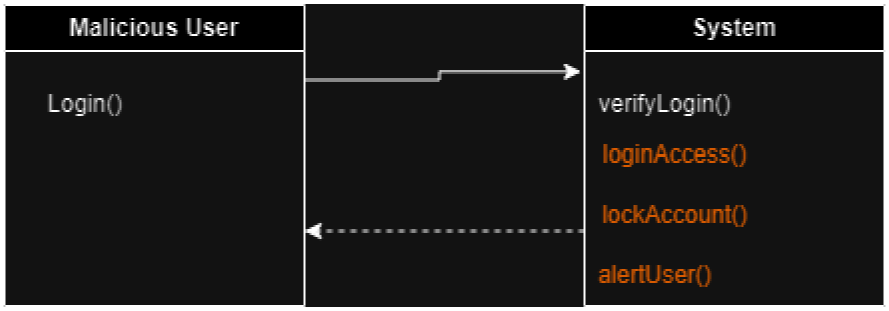
Operation	lockAccount()
Cross-Reference	Brute Force/Dictionary Attack
Precondition	A fifth login attempt has failed
Postcondition	All further attempts are temporarily blocked

Operation	alertUser()
Cross-Reference	Brute Force/Dictionary Attack
Precondition	User account has been locked
Postcondition	An email is sent to the user informing them that their account has been locked

Domain Model



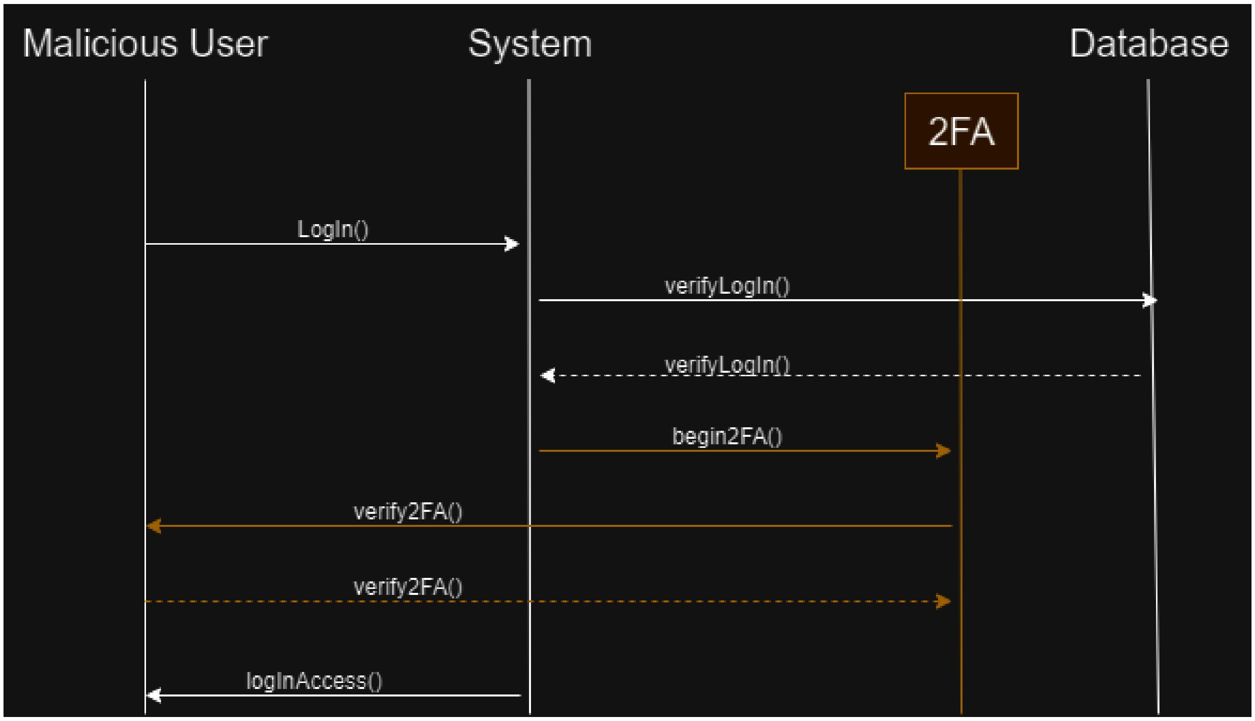
UML Diagram



Abuse Use Case - Stolen Login Information

A Malicious Actor has obtained a user's password and is attempting to gain access to their account and steal sensitive information.

SSD



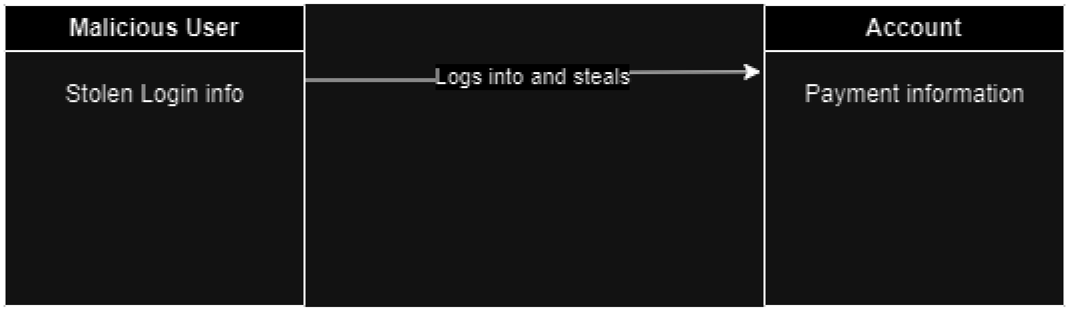
Operation Contracts

Operation	begin2FA()
Cross-Reference	Stolen Login Information
Precondition	Login info has been successfully verified
Postcondition	A 2FA code is generated and emailed to the user

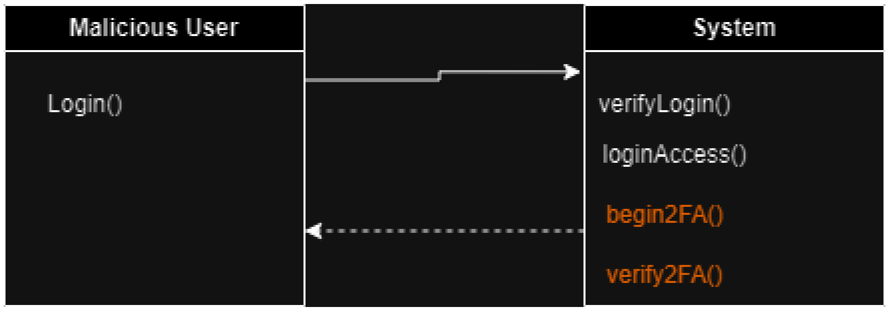
Operation	verify2FA()

Cross-Reference	Stolen Login Information
Precondition	2FA code has been received by the user and input into the system
Postcondition	2FA is verified as valid or invalid

Domain Model



UML Diagram


Malicious User
Login()
System
verifyLogin()
loginAccess()
begin2FA()
verify2FA()