App Components, STRIDE Threats, and Mitigations

Amazon Cognito

Spoofing: Unauthorized users may pretend to be legitimate users. Mitigation: Implement multi-factor authentication.

Tampering: User data could be altered during transmission. Mitigation: Use secure and encrypted connections.

Information Disclosure: Sensitive user data could be exposed to unauthorized users. Mitigation: Encrypt sensitive data.

App Components, STRIDE Threats, and Mitigations

Amazon S3

Tampering: Game assets could be altered. Mitigation: Implement version control and backup systems.

Information Disclosure: Game assets could be exposed to unauthorized users. Mitigation: Use access control lists and bucket policies to restrict access.

Denial of Service: Service could be disrupted, preventing access to game assets. Mitigation: Use AWS Shield for DDoS protection.

App Components, STRIDE Threats, and Mitigations

DynamoDB

Tampering: Game state data could be altered. Mitigation: Implement access controls and monitor activity.

Information Disclosure: Game state data could be exposed to unauthorized users. Mitigation: Encrypt sensitive data.

Denial of Service: Service could be disrupted, preventing updates to game state. Mitigation: Use AWS Shield for DDoS protection.

App Components, STRIDE Threats, and Mitigations

AWS Lambda

Tampering: In-game event processing could be altered. Mitigation: Implement access controls and monitor activity.

Denial of Service: Service could be disrupted, preventing processing of in-game events. Mitigation: Use AWS Shield for DDoS protection.

App Components, STRIDE Threats, and Mitigations

GameLift

Spoofing: Unauthorized users may pretend to be legitimate users in multiplayer events. Mitigation: Implement player authentication and session management.

Denial of Service: Service could be disrupted, preventing multiplayer gameplay. Mitigation: Use AWS Shield for DDoS protection.

App Components, STRIDE Threats, and Mitigations

AppSync

Tampering: Offline play data could be altered during sync. Mitigation: Implement access controls and monitor activity.

Information Disclosure: Offline play data could be exposed to unauthorized users. Mitigation: Encrypt sensitive data.

App Components, STRIDE Threats, and Mitigations

AWS Analytics

Information Disclosure: User behavior and game interaction data could be exposed to unauthorized users. Mitigation: Implement access controls and data anonymization techniques.

App Components, STRIDE Threats, and Mitigations

Amazon Pinpoint

Spoofing: Unauthorized users may send push notifications pretending to be from the app. Mitigation: Implement access controls and monitor activity.

Information Disclosure: User engagement data could be exposed to unauthorized users. Mitigation: Encrypt sensitive data.