This is an auto-generated Threat Modeling Report, assembled by GPT-4 Threat Modeling Agents. The system reviews the specified application architecture. It applies the STRIDE methodology to each component, providing a thorough evaluation of potential security threats, but may still contain errors.

Executive Summary

Executive Summary: This threat modeling exercise has identified the following highest priority items in our application: 1. User authentication via Amazon Cognito: It is critical to ensure secure user authentication to prevent unauthorized access and data breaches. STRIDE threats consist of spoofing (unauthorized user pretending to be an authorized user), tampering (modifying user information), information disclosure (revealing user data) etc. Mitigation strategies should include robust implementation of multi-factor authentication, secure token handling, and encryption of user data. 2. Fetching game assets from Amazon S3: This has potential STRIDE threats of tampering (altering game assets), information disclosure (revealing asset details), and denial of service (making assets unavailable for play). These can be mitigated by ensuring secure access control policies, asset encryption, and regular security auditing. 3. Updating game state in DynamoDB: As DynamoDB is continuously updated, potential threats include tampering (manipulating game state), information disclosure (revealing game state data), etc. Mitigation strategies involve secure access control, data validation techniques, encryption of data, and regular security audits. 4. AWS Lambda functions: Triggered by in-game events, these increase vulnerability to tampering (modifying functions) and denial of service (overloading Lambda functions). Mitigation involves validating function inputs, deploying secure coding practices, and setting rate limits. 5. Multiplayer events via GameLift: This component may face spoofing and denial of service threats. Mitigation can be implemented by secure user verification and adequate capacity planning. 6. User behaviour sent to AWS Analytics: This component is threatened by information disclosure and tampering. Incorporating strong access control and encryption for data transfers are sound mitigation strategies. Constant vigilance, comprehensive threat modeling, and implementing strong security measures for each component can help in significantly lowering the risk associated with these threats.

Results

Component	Threats	Mitigations