Practice Scenarios - Amazon Interview Threat Modeling

Overview

These scenarios mirror actual Amazon Application Security Engineer interview questions. Each includes timing guidelines, expected analysis depth, and sample responses demonstrating Amazon-scale thinking.

Scenario 1: Prime Video Streaming Platform

Interviewer Setup (2 minutes)

> "Amazon Prime Video serves 200+ million subscribers globally, streaming millions of hours of content daily. The platform includes user accounts, content catalogs, streaming servers, payment processing, and content recommendations. Walk me through how you would threat model this system."

Time Allocation (18 minutes total)

- **Architecture Understanding** (3 minutes)
- **STRIDE Analysis** (12 minutes)
- **Customer Impact & Mitigations** (3 minutes)

Expected Response Framework

Architecture Mapping (3 minutes)

High-Level Components:

```
[Users] → [CloudFront CDN] → [API Gateway] → [Microservices]
                                              ↓
[Content Storage] ← [Transcoding Pipeline] ← [User Management]
       ↓                    ↓                      ↓
[DRM Systems] → [Analytics] → [Recommendation Engine]
```

Trust Boundaries Identified:

1. Internet users → AWS infrastructure
2. Public APIs → Internal microservices
3. User data services → Content delivery systems
4. Payment processing → Account management
5. Content ingestion → Content distribution

STRIDE Analysis (12 minutes)

Spoofing (2 minutes)

Primary Threats:

- Account takeover through credential stuffing
- Content piracy through subscriber sharing
- API impersonation for unauthorized access

Amazon Scale Impact:

> "With 200M subscribers, credential stuffing affects 0.1% = 200K accounts potentially compromised monthly. Each compromised account represents $120 annual revenue loss + $50 remediation cost = $34M annual impact from this threat alone."

Mitigations:

- Multi-factor authentication for high-value accounts
- Device fingerprinting and behavioral analytics
- Rate limiting and geographic anomaly detection

Tampering (2 minutes)

Primary Threats:

- Video content modification during delivery
- User preference manipulation affecting recommendations
- Billing data tampering

Customer Impact Analysis:

> "Content tampering affects customer experience quality, leading to 15% higher churn rates for affected viewers. With average customer lifetime value of $1,400, each lost customer due to content quality issues costs $1,400 + $200 acquisition cost replacement = $1,600 total impact."

Mitigations:

- Content integrity verification using checksums
- Encrypted content delivery with DRM
- Immutable audit trails for user data changes

Repudiation (2 minutes)

Primary Threats:

- Users denying subscription charges
- Content providers denying licensing agreements
- Admins denying configuration changes

Business Impact:

> "Payment disputes affect 2% of transactions annually. With $8B Prime Video revenue, 2% disputes = $160M annual dispute resolution costs, plus regulatory compliance overhead."

Information Disclosure (2 minutes)

Primary Threats:

- User viewing history exposure
- Content catalog leaks before release
- Payment information disclosure

Regulatory Impact:

> "Under GDPR, viewing history exposure for EU customers could trigger up to €20M fine. Additionally, 67% of customers report they would cancel service if viewing history was exposed, representing massive customer trust erosion."

Denial of Service (2 minutes)

Primary Threats:

- CDN overload during popular content releases
- Database exhaustion from recommendation queries
- Payment processing system overload

Revenue Impact Calculation:

> "During 'The Boys' season finale, 50M concurrent viewers generate $2.3M hourly ad revenue. 4-hour outage = $9.2M direct loss + $25M customer credits + competitive reputation damage."

Elevation of Privilege (2 minutes)

Primary Threats:

- Content management system privilege escalation
- Cross-tenant access in multi-tenant infrastructure
- Admin panel unauthorized access

Critical Impact Assessment:

> "Admin access compromise could enable content deletion affecting all 200M subscribers. Recovery from complete content catalog loss: 72+ hours, $500M+ revenue impact, permanent brand damage to 'reliability' reputation."

Customer Impact & Mitigations Summary (3 minutes)

Top 3 Customer Trust Risks:

1. **Account Security**: MFA implementation prevents 95% of account takeovers
2. **Content Quality**: Integrity verification ensures consistent viewing experience
3. **Service Availability**: Multi-region deployment with 99.99% availability SLA

Amazon-Scale Mitigations:

- **AWS WAF**: Application layer protection with custom rules
- **GuardDuty**: Threat detection across all AWS services

- **Security Hub**: Centralized security finding management
- **CloudTrail**: Comprehensive audit logging for compliance

Scenario 2: Alexa Voice Assistant Platform

Interviewer Setup

> "Alexa processes billions of voice commands monthly from 100+ million devices globally. The system includes voice recognition, natural language processing, third-party skills, and smart home integration. How would you approach threat modeling this platform?"

Expected Analysis Depth

Privacy-First Threat Analysis

Unique Considerations:

- Voice data contains biometric identifiers
- Always-listening devices in private spaces
- Third-party skill ecosystem security
- Cross-device synchronization vulnerabilities

Customer Trust Specific Threats

Voice Privacy Concerns:

> "Unauthorized voice recording affects customer intimacy and privacy. Research shows 73% of customers would stop using voice assistants if personal conversations were exposed. With 100M active devices, loss of 73M customers = $87B lifetime value impact."

Smart Home Integration Risks:

> "Compromised Alexa device enables home automation control. Physical security breach through digital attack vector creates liability concerns and potential physical harm to customers and families."

Sample Mitigation Strategy

Privacy by Design Implementation:

- Local processing for sensitive commands
- Encrypted voice storage with automatic deletion
- Explicit user consent for data sharing
- Third-party skill security certification program

Scenario 3: AWS Marketplace Platform

Interviewer Setup

> "AWS Marketplace allows software vendors to sell applications to AWS customers. The platform handles software listings, customer purchases, license management, and revenue sharing. Threat model this multi-sided marketplace."

Multi-Stakeholder Threat Analysis

Three-Way Trust Model

Stakeholders:

1. **Software Vendors**: Want secure IP protection and reliable payments
2. **AWS Customers**: Need secure software and billing transparency
3. **Amazon**: Responsible for platform security and revenue collection

Unique Threat Categories

Supply Chain Security:

- Malicious software uploaded by vendors
- Legitimate software compromised during distribution
- License key generation and validation vulnerabilities

Financial Trust Threats:

- Revenue sharing calculation manipulation
- Payment routing vulnerabilities
- Cross-customer billing errors

Customer Impact Framework:

> "Malicious software affects enterprise customers managing critical infrastructure. One compromised enterprise customer could cascade to millions of end-users. Enterprise customer average value $2M annually - single major incident could trigger $50M+ customer departures."

Scenario 4: Amazon Pay Platform

Interviewer Setup

> "Amazon Pay allows customers to use their Amazon accounts to pay on external merchant websites. The system handles payment authorization, fraud detection, merchant onboarding, and dispute resolution. Walk me through your threat modeling approach."

Financial Services Threat Model

Regulatory Compliance Integration

PCI DSS Requirements:

- Card data handling and storage restrictions
- Regular security testing and validation

- Vendor management for third-party processors

Cross-Platform Trust:

> "Amazon's brand reputation extends to merchant sites using Amazon Pay. Security incident at merchant site reflects on Amazon's security posture. Protecting 300M+ customer payment methods requires zero-trust architecture for all external integrations."

Fraud Detection Scale Challenges

Real-Time Processing:

- 50,000+ transactions per second during peak periods
- Machine learning model accuracy under adversarial attacks
- False positive impact on legitimate customer transactions

Quick Practice Framework (5-Minute Scenarios)

Rapid Threat Identification Process

1. **30 seconds**: Draw basic architecture
2. **2 minutes**: Identify top 3 threats with highest customer impact
3. **1.5 minutes**: Propose AWS-native mitigations
4. **1 minute**: Quantify business impact in customer/revenue terms

Speed Practice Scenarios

Scenario A: S3 Public File Sharing

Threat: Public bucket misconfiguration **Customer Impact**: Customer data exposure → $165/record × affected customers **Mitigation**: S3 Block Public Access + automated compliance checking

Scenario B: Lambda Function Processing

Threat: Code injection through event data **Customer Impact**: Service disruption affecting dependent applications **Mitigation**: Input validation + least privilege IAM roles

Scenario C: RDS Customer Database

Threat: SQL injection enabling data exfiltration **Customer Impact**: Complete customer database compromise **Mitigation**: Parameterized queries + database activity monitoring

---

Interview Success Patterns

Consistently Successful Responses Include:

1. **Systematic Methodology**: Clear STRIDE or similar framework application
2. **Scale Awareness**: Amazon's global user base considerations
3. **Customer Obsession**: Every threat connected to customer impact

4. **Business Quantification**: Specific dollar amounts and metrics
5. **AWS Integration**: Native AWS services for scalable solutions
6. **Regulatory Awareness**: Compliance implications (GDPR, PCI, HIPAA)

Common Interview Pitfalls to Avoid:

1. **Generic Analysis**: Not considering Amazon's specific scale and requirements
2. **Technical Only**: Missing business impact and customer trust implications
3. **Unrealistic Solutions**: Proposing mitigations that don't scale to Amazon's size
4. **Missing Follow-up**: Not preparing for deeper questions about proposed solutions

Interviewer Follow-up Preparation

Expected Deep-Dive Questions:

- "How would you implement that mitigation at Amazon's scale?"
- "What metrics would you use to measure the success of that security control?"
- "How would you communicate this threat to non-technical stakeholders?"
- "What would be the customer communication strategy if this threat materialized?"

Advanced Scenarios:

- Multiple simultaneous attacks
- Zero-day vulnerabilities in core systems
- Compliance failures during critical business periods
- Cross-service security dependencies

This comprehensive practice framework ensures you can demonstrate the systematic thinking, business acumen, and Amazon-scale perspective required for the Application Security Engineer role.