Serverless Application Security

Marcin Hoppe @ infoShare 2019

Ground Rules

Marcin Hoppe

- ➔ Product Security Manager at Auth0
- ➔ Security Working Group at Node.js Foundation
- ➔ OWASP Serverless Top 10

E-mail @ marcin.hoppe (at) {acm.org, owasp.org}

Organization

- Breaks
- Questions
- Exercises

Agenda

1. AWS Lambda Security Fundamentals
2. Authentication and Authorization
3. Secrets Management
4. Protecting Web Applications

AWS Lambda Security Fundamentals

AWS Lambda Security Model

Security of the cloud (AWS)

- Data centers and edge locations
- Compute, storage, network resources
- Operating systems
- Platform management (isolation!)
- Identity and Access Management

Security in the cloud (you)

- Infrastructure access control
- Application security
- Data management
- Identity and Access Management

AWS Lambda Runtime Isolation

- Control plane and data plane
- Lambdas run in MicroVMs
  - Isolation mechanisms: cgroups, namespaces, seccomp-bpf, iptables, chroot
- MicroVMs are not shared across accounts
- Shared storage: `/tmp`
- Memory scrubbing

AWS Lambda Permissions

- Invocation permissions
- Execution roles
- Resource-based policies
- Identity-based policies

- Role-per-function
- Least privilege
- No wildcards
  - Actions
  - Resources

Monitoring and Auditing

- AWS CloudWatch
- AWS CloudTrail
  - AWS GuardDuty
- AWS X-Ray
- AWS Config
- SIEM
  - ELK, SumoLogic, Splunk, etc.

Lab 1: Setup

Practice!

Authentication and Authorization

AuthN and AuthZ

Authentication

- Verify identity
- Users
- Applications and services
- Credentials

Authorization

- Principal + action + resource
- RBAC
- ABAC
- OAuth 2.0 scopes

Protocol Zoo

- OAuth 2.0
  - Authorization Code (+ PKCE)
  - Implicit
  - Client Credentials
  - Resource Owner Password
- OpenID Connect
  - Hybrid
- SAML

Tokens

- Access tokens
- ID tokens
- Refresh tokens
- Formats
  - JSON Web Tokens (JWT)
  - Opaque (reference)
- Claims

Identity Providers

- AWS Cognito
- Auth0, Okta, OneLogin, etc.
- Social providers
  - Google
  - Facebook
  - Twitter
- User directories (e.g. Active Directory)

API Gateway Authorizers

- Input can be a bearer token or query parameters
- Output is a principal and an IAM policy
- Policy caching
- Integration with AWS Cognito
- Pattern: authorizers centralized in a security account

Lab 2: Authentication with Auth0

Practice!

Secrets Management

Cloud Key Management

Keys

- Generation
- Storage
- Rotation
- Audit

Data

- Encryption
- Signature
- MAC
- Secrets and credentials

AWS Key Management Service

Operations

- GenerateRandom / GenerateDataKey
- Encrypt / Decrypt / ReEncrypt
- Key operations
  - Enable / disable / rotate
- Authenticated encryption
  - AES in GCM mode

Keys

- Customer Master Keys (CMK)
  - Customer managed
  - Imported
  - AWS Managed
- Customer Data Keys (CDK)

AWS Lambda Secrets Management

- Encrypted environment variables
- EC2 Systems Manager Parameter Store
- Secrets Manager
- All use KMS under the hood!
- Bring-your-own: HashiCorp Vault

Lab 3: Secrets

Practice!

Protecting Web Applications

API Gateway

- Resource policies
- IAM roles and policies
- CORS
- Authorizers: Cognito & custom (Lambda)
- mTLS
- API keys and usage plans

AWS WAF Filters

- Cross-site scripting (XSS) and SQL injection (SQLi)
- Strings and regular expressions
- IPs
- Geo-based
- Size-based
- Rate-based rules

AWS WAF Deployment

- AWS API Gateway
- AWS Application Load Balancer (ALB)
- AWS CloudFront
- Manage with AWS Firewall Manager

Lab 4: API Gateway and WAF

Practice!

Cleanup

- `claudia destroy` - authorizer & tasks-api
- DynamoDB
- WAF
- IAM
- CloudWatch

Resources

- OWASP Cloud Security
- OWASP DVSA & Serverless Goat
- OWASP Serverless Top 10
- Commercial: PureSec and Protego

Survey

Thanks!

Thanks!

Contact:

Marcin Hoppe

marcin.hoppe@acm.org
marcin.hoppe@owasp.org