Post Quantum Cryptography in the Cloud

Ken Beer
General Manager – AWS Key Management Systems and Crypto Tools
AWS Cryptography
AWS Cryptography – What we do

External Customers

Web Services

• AWS Key Management Service
• AWS CloudHSM
• AWS Certificate Manager/Private CA
• AWS Secrets Manager
• s2n - TLS
• AWS Encryption SDK
• DynamoDB Encryption Client
• S3 Encryption Client

Internal Developers

Developer Tools

• AES optimization
• Hybrid-PQ key exchange
• Privacy preserving encryption

Research and Development
Cryptography across the lifecycle of customer data

- TLS session key negotiation when calling an AWS API
- Optional VPN tunneling
- API signatures
- Temporary API signing credentials with automatic rotation
- VPC encryption between customers’ compute instances
- At rest encryption for all AWS services
- Certificate generation, issuance, deployment, rotation
- Arbitrary secrets management

Over 250 million cryptographic operations per second across all AWS infrastructure
Allowing customers to maintain crypto agility

AWS Key Management Service

• Extending AES-GCM to $2^{50}$ operations under a single 256-bit key

• Import Key - customers control generation of secret key material

• Custom Key Store – AWS common authN and authZ to customer-controlled CloudHSM instances

AWS Certificate Manager

• Free generation, deployment and rotation of publicly trusted certificates

• AWS automatically migrates customers to new algorithms and protocols
Customer challenges for cryptography at scale

**Configuration**
- How to enforce use of encryption/signing with the parameters you want?
- Trust models when service A delegates to service B to service C to service D...

**Monitoring**
- What does a cryptographic compromise look like?
- Are your cryptographic services scaling with you read/write rate?

**Remediation**
- How do you return to a state of forward secrecy?
- How much do you trust your cloud provider to remediate potential problems?
Amazon challenges for cryptography at scale

**Configuration**
- How to enable 100s of development teams to innovate quickly without lowering the security bar?

**Monitoring**
- How to verify customers are applying best practices when we can’t know how their data is classified?

**Remediation**
- How to upgrade crypto primitives across 100,000s of packages as needed?
The quantum opportunity

We see quantum computing as a niche computing capability that our customers will want to use in the future and pay for as they go.

It will likely come in the form of some type of special co-processor capable of doing special computations in fields like molecular modeling and complex simulations.

Classical computing will still play a role to manage inputs and outputs of quantum computing systems.

*The security level of data passing within and between classical and quantum computing systems must be maintained*
One known risk quantum computing brings to Amazon customers

plaintext data

Record and harvest

New capabilities

Internet

Client

AWS Cloud

Amazon S3

Amazon Aurora

Amazon EC2

Amazon SageMaker

Amazon DynamoDB
Amazon commitment to quantum-safe cryptography

- Supporters of the ETSI-IQC Quantum Safe Cryptography Workshop since 2013
- Member of the ETSI Quantum Safe Cryptography Technical Committee
- Contributing to two proposals to NIST's PQC Standardization process (BIKE and SIKE)
- Supporter of the libOQS project at the University of Waterloo
Amazon delivery in quantum-safe cryptography

Hybrid key agreement scheme

- Executes two independent key exchanges and feeds the two resulting shared secrets into a Pseudo Random Function (PRF), with the goal of deriving a secret which is as secure as the stronger of the two key exchanges.

- Implementation using BIKE and SIKE with ECDHE in a TLS 1.2 handshake.

- Available in s2n project at https://github.com/awslabs/s2n/tree/master/pq-crypto
Amazon delivery in quantum-safe cryptography

You can use the hybrid key agreement scheme today

Deployed to over all non-FIPS 140-2 validated KMS service API endpoints in commercial regions (over 1,000 endpoints)
  • We are asking for data on the effects of longer TLS handshake times and larger key exchange messages in real-world customer environments

Integrated as developer preview of our AWS Java SDK 2.0
Thank you!

Ken Beer
kenbeer@amazon.com