Traffic Protection

Steven Moran
TECHNICAL INSTRUCTOR

Cryptography - Protecting Data Since 1500 BC.

Secure data transmission requires:

- Verifying the identity of the recipient
- Encrypting transmitted data

How do strangers establish this?

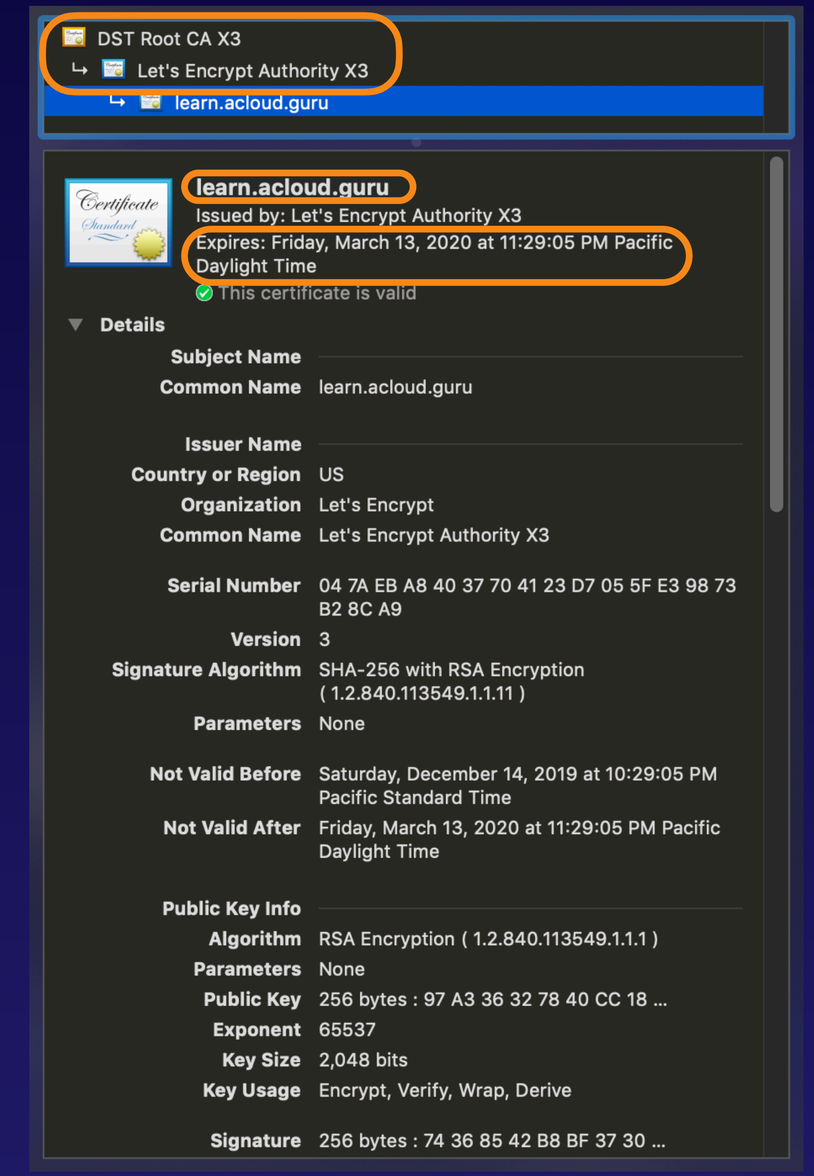
Public Key Infrastructure

- PKI is a collection of systems used to verify identities and secure electronic data transfer.

- **Certificates** are used by PKIs to verify identities and ownership of encryption keys.

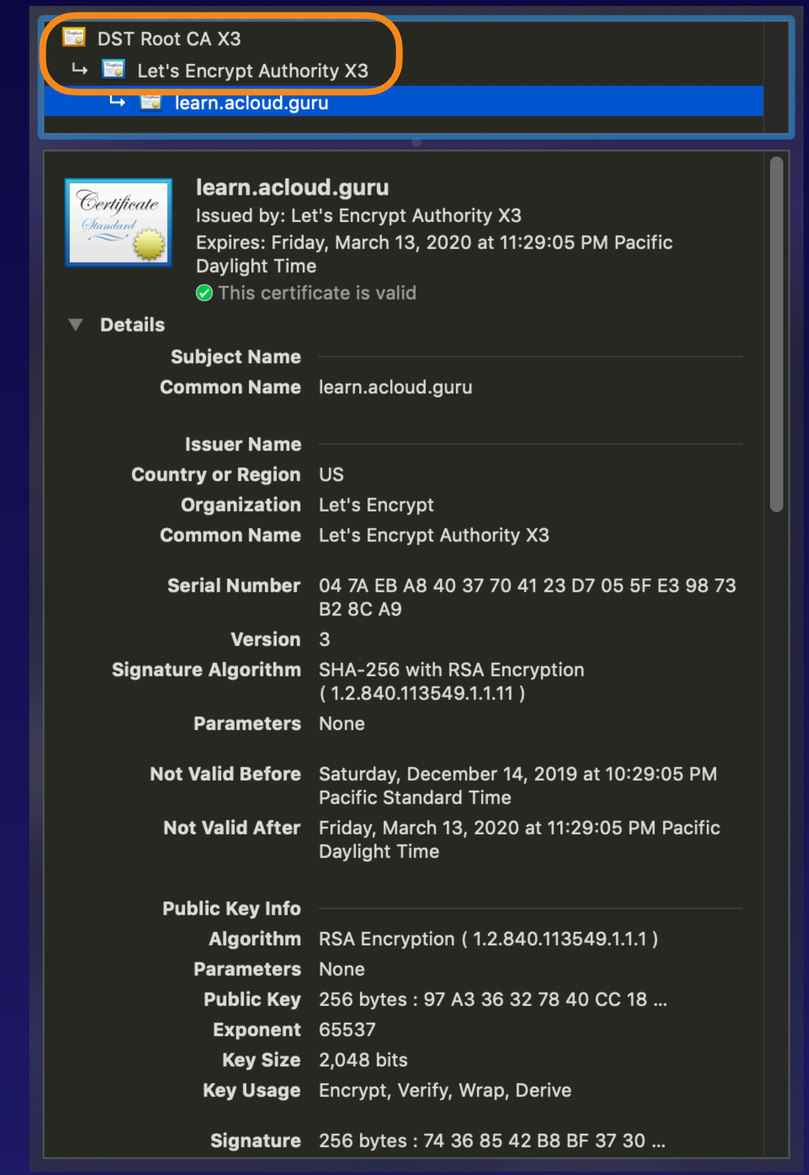
Digital Certificates

- Certificates contain information to validate the identity of both the holder of the certificate as well as the issuer of the certificate:
  - Name of the certificate holder
  - Other information about the holder
  - Purpose of the certificate
  - Expiration date
  - Identity of the issuer
  - Means of validating the authenticity of the certificate



Digital Certificates

- Trust in the issuing certificate authority (CA) chain is required.
- Servers use certificates used by public CAs to prove their identity to requesting clients.
- If there are any problems in validating the certificates in the chain, the associated operation will be rejected.



SSL/TLS (Secure Sockets Layer/Transport Layer Security)

- SSL/TLS are protocols used to establish secure network communications.
- SSL depreciated in 2015.
- AWS recommends using TLS 1.2 wherever possible.

AWS Certificate Manager (ACM)

- Certificates in AWS can be managed using either ACM or IAM.
  - ACM not available in all regions.
  - IAM cannot be used to create certificates.
  - ACM certificates cannot be imported by IAM.
  - IAM certificates cannot be managed from the Console.
- Integrated with AWS services:
  - ELB
  - CloudFront
  - API Gateway
  - CloudFormation
  - Elastic Beanstalk

AWS Certificate Manager (ACM)

- Provision public certificates.
  - SSL/TLS for public services
  - Import external X.509 certificates
  - Provisioned from AWS CA
  - Free service
- Requires validation of domain ownership:
  - FQDN of website (* wildcard accepted)
  - Validate via:
    - DNS (add text record to zone)
    - Email (automatically sent to zone contacts)
- Certificate format is X.509 v3.
- Valid for 13 months.

AWS Certificate Manager (ACM)

- Certificates are provisioned on a per-region basis.
- Certificates used by CloudFront must be provisioned in us-east-1.
- ACM certificates can only be used by AWS services integrated with ACM.
- ACM certificates and their private keys may not be downloaded.

AWS Certificate Manager Private Certificate Authority (ACM PCA)

- Create your own private CA infrastructure.
  - SSL/TLS certificates to identify internal resources
  - $400/month per CA
  - Charge per private certificate

What Needs to Be Protected?

- Requests from external clients to AWS services.
- Traffic within AWS.

Protecting client requests - CloudFront

- Settings configured per cache behavior
- Viewer Protocol Policy
  - HTTP and HTTPS (default)
  - Redirect HTTP to HTTPS
    - Tells client to submit new request to HTTPS URL
    - Requests below HTTP v1.1 will be rejected (status 403 Forbidden)
  - HTTPS only
    - All HTTP requests will be rejected (status 403 Forbidden)

Protecting client requests - CloudFront

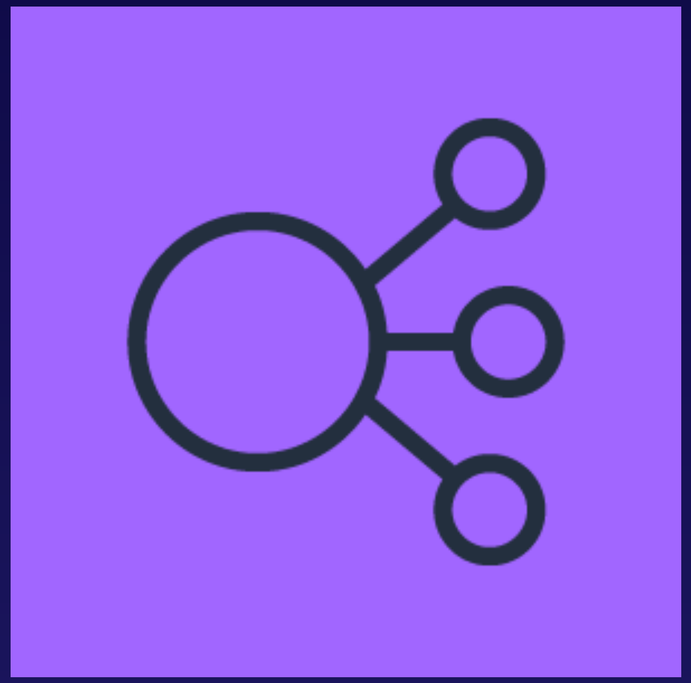
- Settings configured per cache behavior
- Viewer Protocol Policy
  - HTTP and HTTPS (default)
  - Redirect HTTP to HTTPS
  - HTTPS only
- SSL Certificate
  - Default CloudFront certificate
    - Requests must use CF domain name
    - Only supports TLSv1 or later
  - Custom SSL certificate
    - Requests use custom domain name
    - Certificates must be in either ACM (us-east-1) or in IAM

Protecting client requests - S3

- Deny connections not using HTTPS via bucket policy condition.

```
{
  "Sid": "AllowSSLRequestsOnly",
  "Action": "s3:*",
  "Effect": "Deny",
  "Resource": [
    "arn:aws:s3:::awsexamplebucket",
    "arn:aws:s3:::awsexamplebucket/*"
  ],
  "Condition": {
    "Bool": {
      "aws:SecureTransport": "false"
    }
  },
  "Principal": "*"
}
```

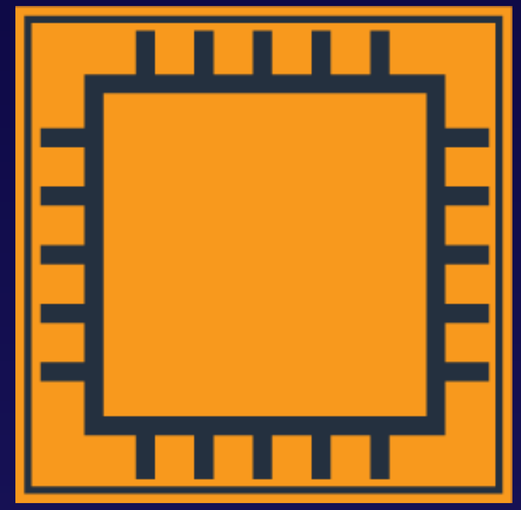
Protecting client requests - ELB

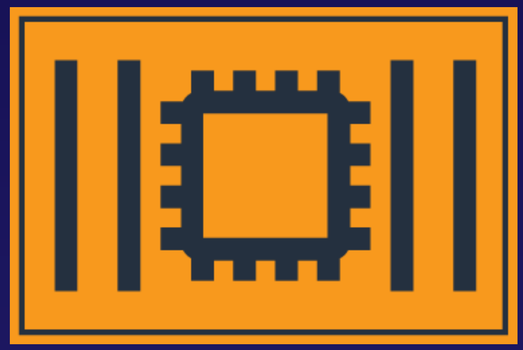


- Configure a listener for a secure protocol:
  - CLB - HTTPS or SSL
  - ALB - HTTPS only
  - NLB - TLS only
- Select default certificate and security policy.
  - CLB may modify policy details in Console.
  - ALB and NLB may add additional certificates after creation.
  - Default certificate is used when:
    - Client doesn't connect with SNI support.
    - Requested hostname does not match any additional certificates.

Protecting client requests – EC2 and Container Instances

- Enabling HTTPS/TLS at ELB terminates secure session at ELB.
- Configure CLB/NLB listener for TCP.
- Route traffic to appropriate port on application instance.

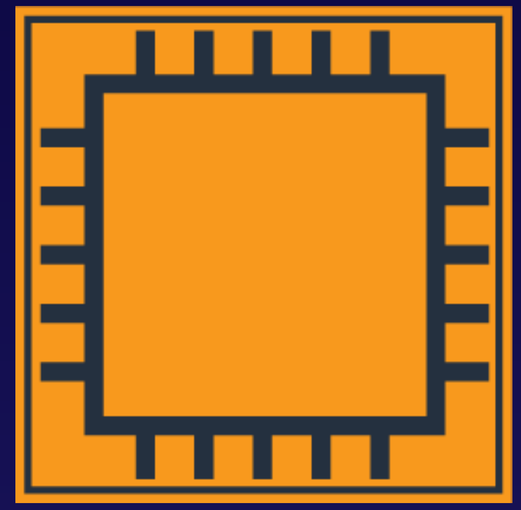


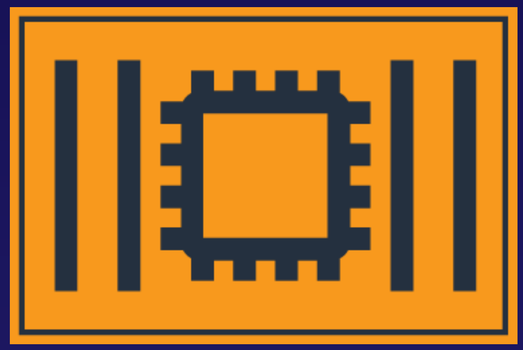


Protecting client requests – EC2 and Container Instances

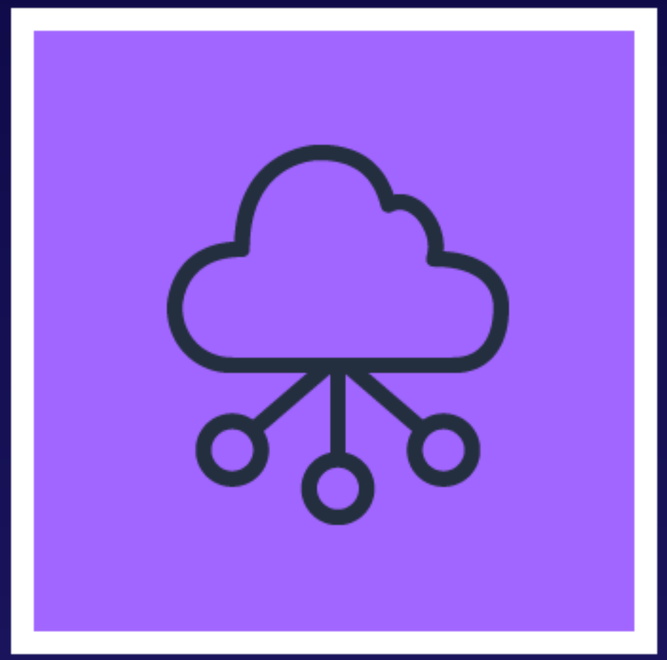
- Services hosted on instances are the customer's responsibility to configure and maintain.

- Handling SSL/TLS connections at application server increases resource consumption.





Protecting Intra-AWS traffic

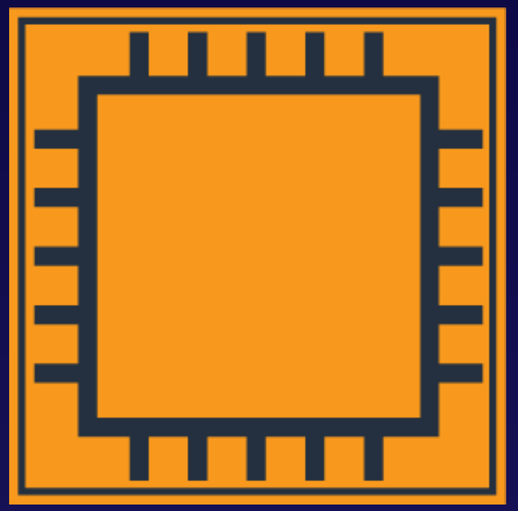


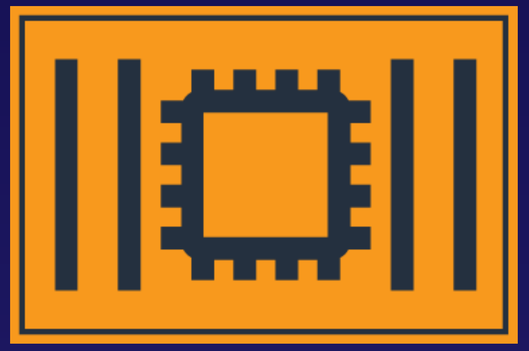
- AWS network traffic uses shared infrastructure.
- AWS service objects provisioned in AWS may be hosted on hardware in different locations.
- Organizational compliance requirements might require secured connections to customer-managed services.

Protecting Intra-AWS traffic - CloudFront

- Settings configured per origin
- Origin Protocol Policy
  - HTTP Only (default)
  - HTTPS Only
  - Match Viewer
- Origin-type specifics:
  - Certificate at custom origin servers must be from a Mozilla-trusted CA
  - S3 bucket origins are always “Match Viewer”
    - Configure Viewer Protocol Policy
  - S3 buckets as websites do not support HTTPS

Protecting Intra-AWS traffic - EC2 and Container Instances

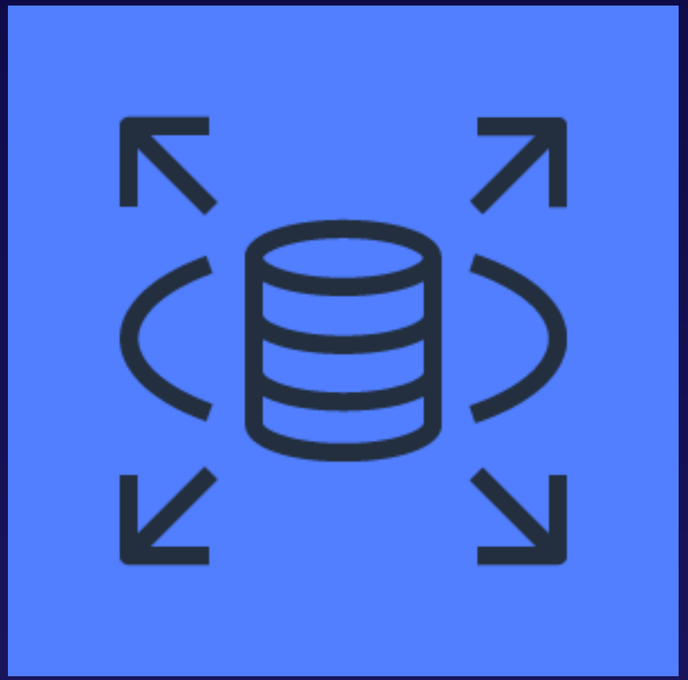




- Secured network connections in-between instances require OS-level service configuration.
- EBS encryption encrypts data traffic between instance and EBS volumes.
- EFS traffic can be secured by TLS when volumes are mounted (per connection).
- FSx traffic is automatically encrypted when accessed using SMB 3 or Samba 4.2 (or newer).

Protecting Intra-AWS traffic - RDS

- RDS creates an SSL/TLS certificate and installs the certificate on the provisioned DB instance.
- Methods of requiring SSL/TLS connections vary by DB engine and version.
- AWS root certificates for RDS will need to be applied to clients.



What About Encryption at Rest?

- Data can be encrypted at different locations:
  - Client
  - AWS service
  - Customer service
- AWS services for customer key management:
  - Key Management Service (KMS)
    - Integrated with many AWS services
    - Allows granular access controls
    - Shared infrastructure
  - CloudHSM
    - AWS-managed HSM appliance
    - Not integrated with AWS services

Fast Takeaways

Using AWS-managed services shifts responsibility towards AWS.

Require SSL/TLS use wherever possible.

Encrypting data in motion does NOT encrypt data at rest.