CPSL

Cyber-Physical Systems Laboratory

AWS IoT Tutorial

Haoran Li

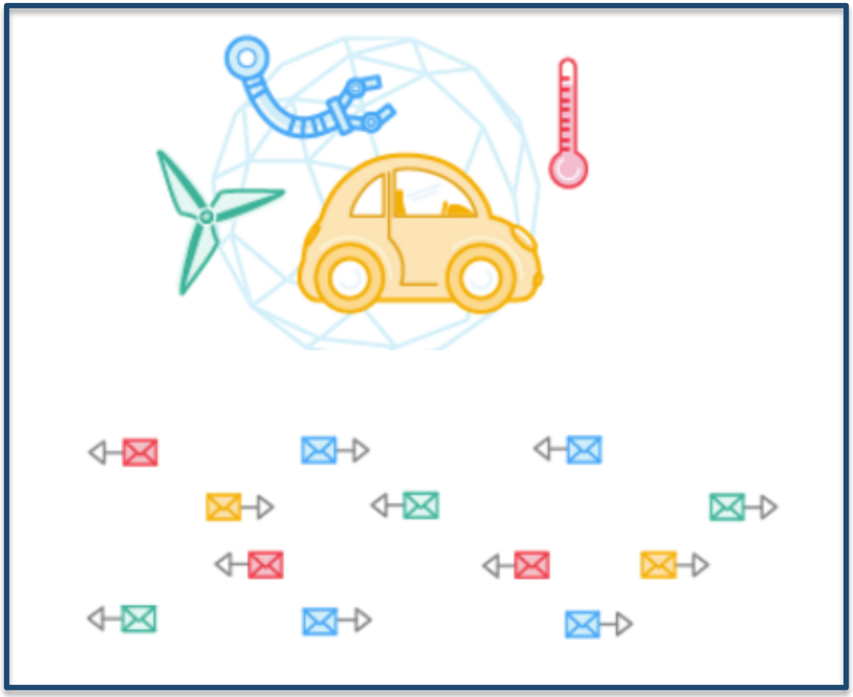
TA for class CSE 521S, Spring

1/19/2017

Washington University in St. Louis

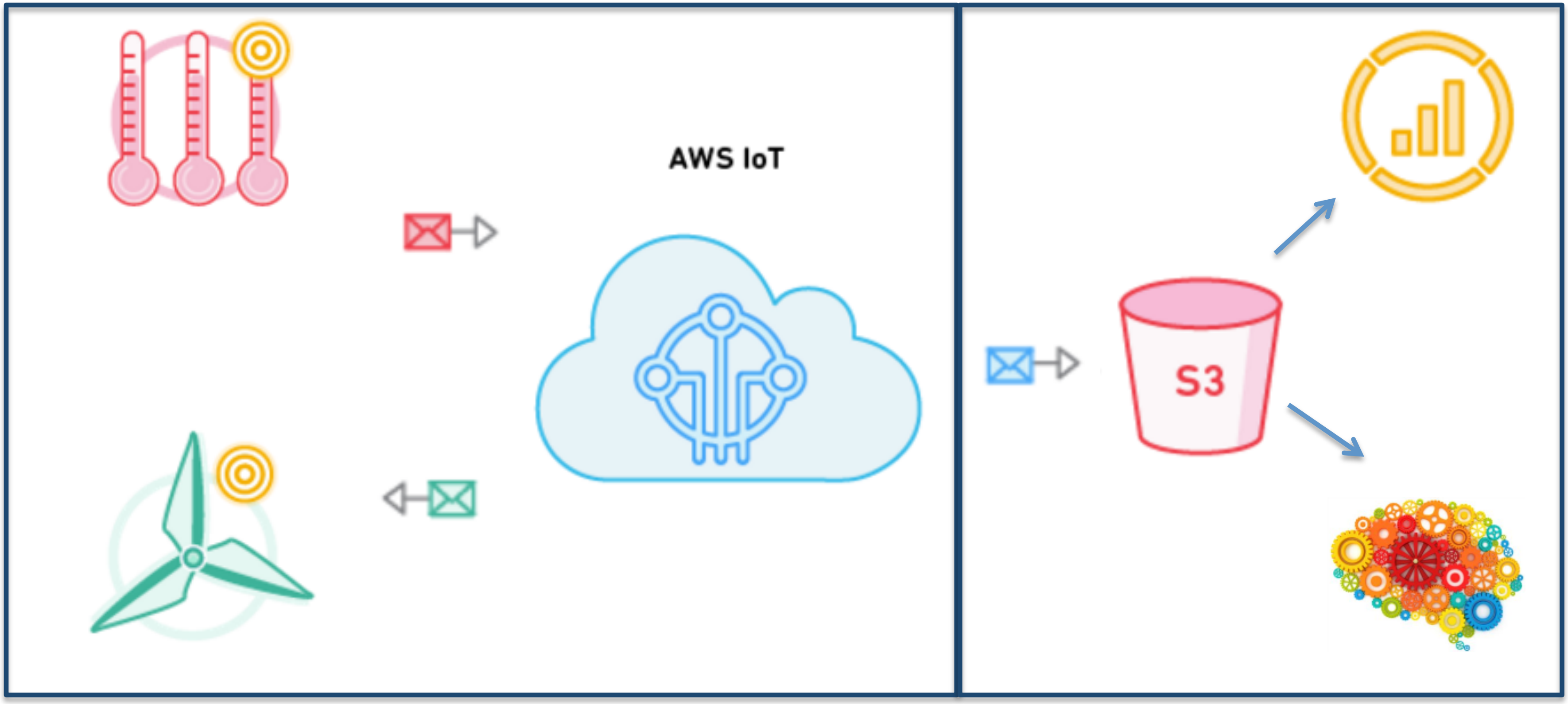
Internet-of-Things

- Things (Devices)
  - Many of them
    - Different Types
    - Isolated Systems
  - Data and Command
    - Sensing the world
    - Give Response
  - Challenge
    - United: Connected + Communication
    - Smart: Data Analytics + Strategy



Source: https://aws.amazon.com/iot-platform/
http://www.brain-smart.net/smart-brain-health-blog/page/2/#axzz4W4oSp8a6

Solution: AWS IoT

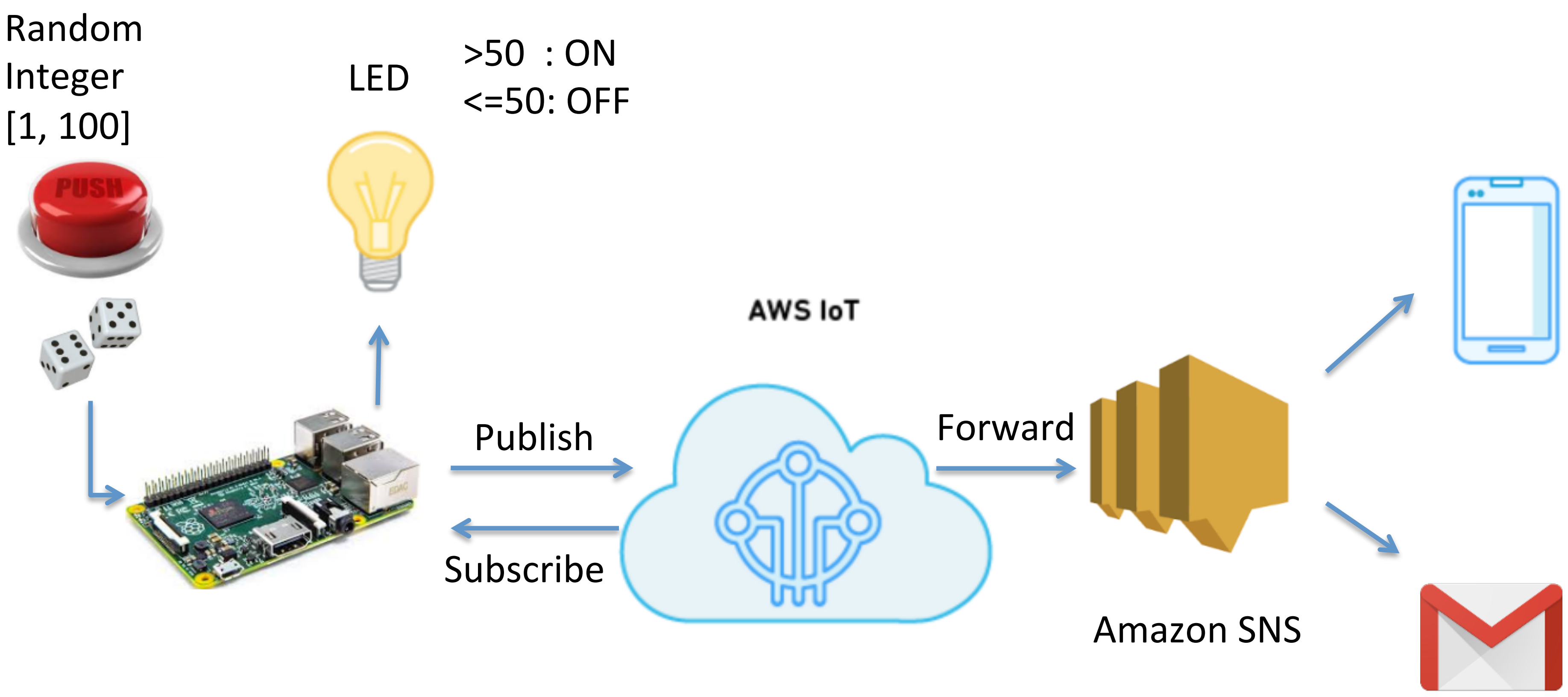


United: Connect + Communication

Smart: Other Cloud Service
Data Storage
Machine Learning

Source: https://aws.amazon.com/iot-platform/

Tutorial: Hello AWS IoT!



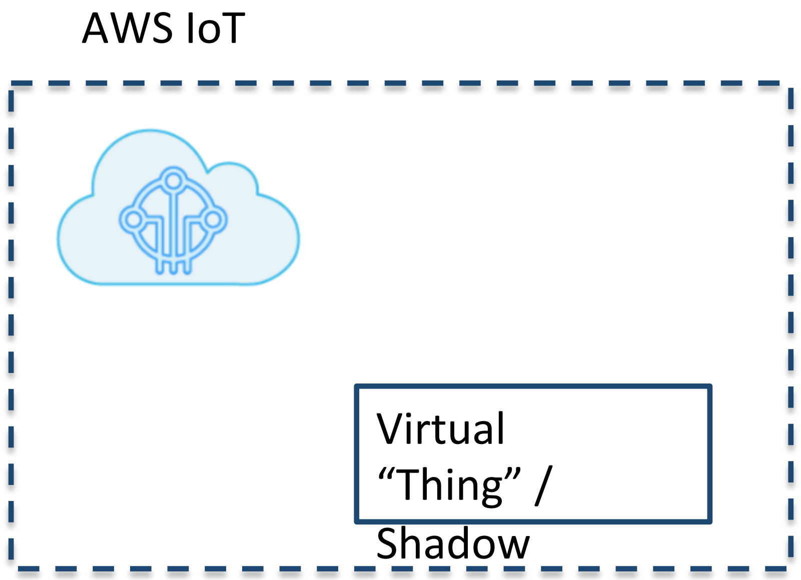
Random Integer [1, 100]

LED

>50 : ON
<=50: OFF

Source: https://aws.amazon.com/iot-platform/

Step 1: Create a Virtual "Thing”

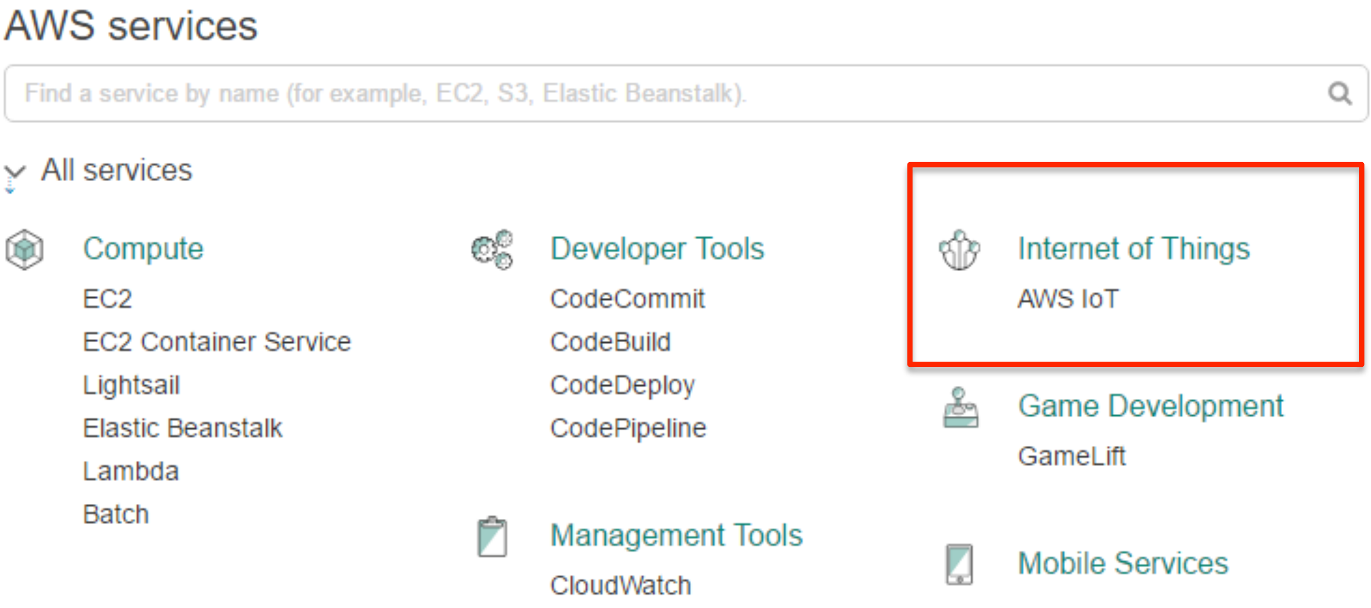


AWS IoT

Virtual “Thing” / Shadow

Get into AWS Manage Console

- Create your own AWS account
- Sign In IoT Manage Console
  - □ https://aws.**amazon**.com/**iot**/



AWS services

Find a service by name (for example, EC2, S3, Elastic Beanstalk).

All services

Compute
- EC2
- EC2 Container Service
- Lightsail
- Elastic Beanstalk
- Lambda
- Batch

Developer Tools
- CodeCommit
- CodeBuild
- CodeDeploy
- CodePipeline

Management Tools
- CloudWatch

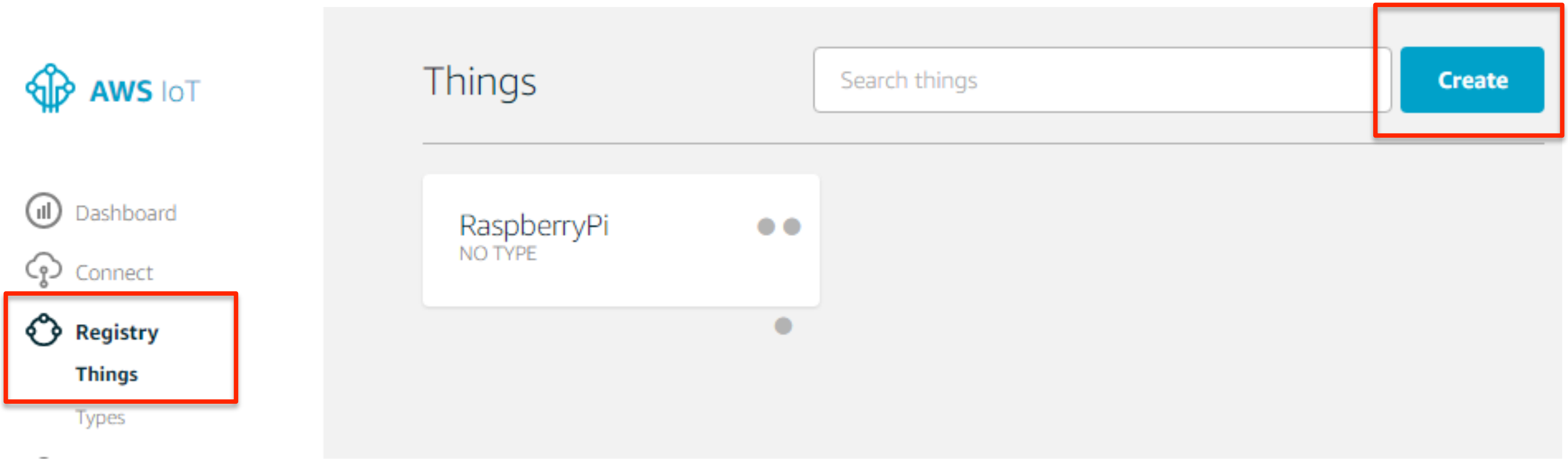
Internet of Things
- AWS IoT

Game Development
- GameLift

Mobile Services

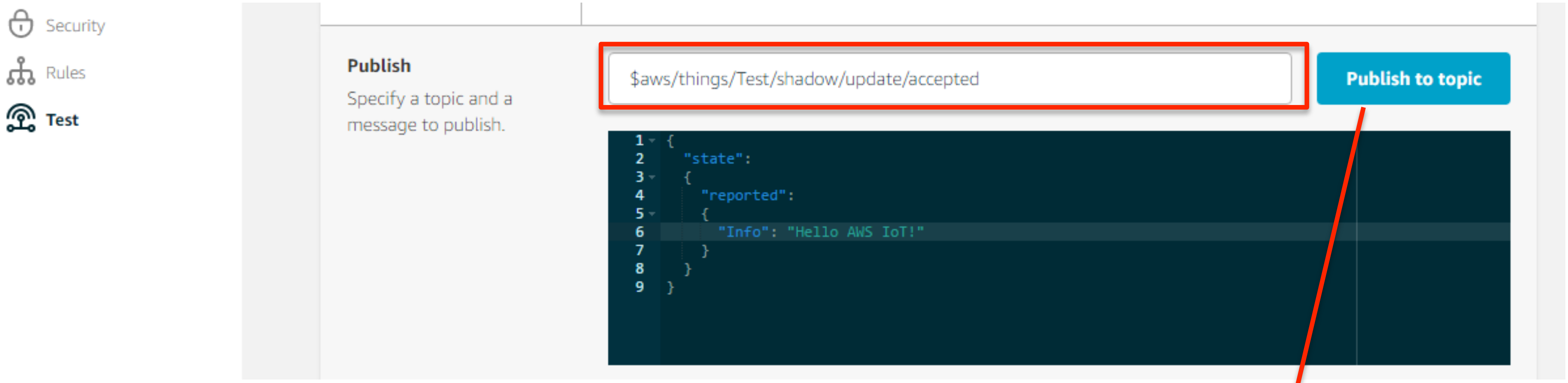
Create a thing

- 1. AWS IoT Menu
  - ❑ Registry
    - Things ➔ Create
- 2. Give a name



Basic Interact: Publish

- Using Embedded **MQTT Client** to Test



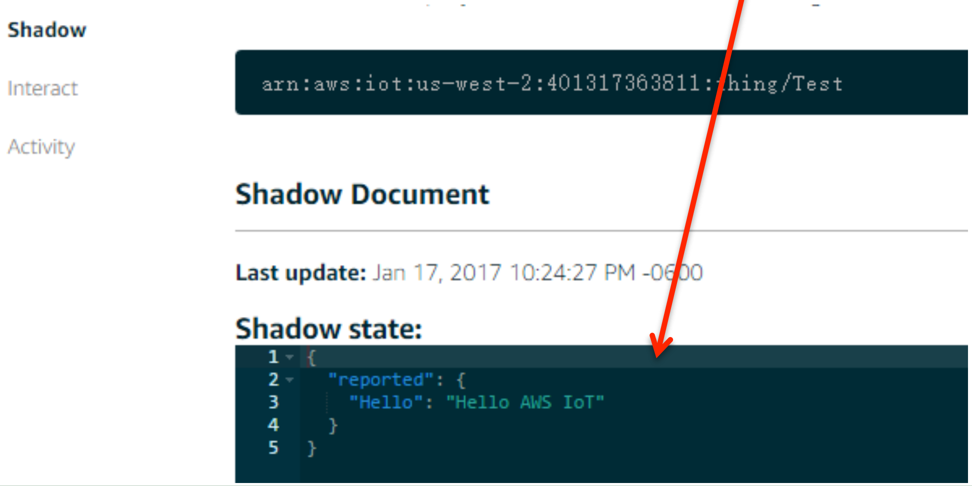
Publish

Specify a topic and a message to publish.

$aws/things/Test/shadow/update/accepted

```
{
  "state":
  {
    "reported":
    {
      "Info": "Hello AWS IoT!"
    }
  }
}
```

- Check the Things Shadow



arn:aws:iot:us-west-2:401317363811:thing/Test

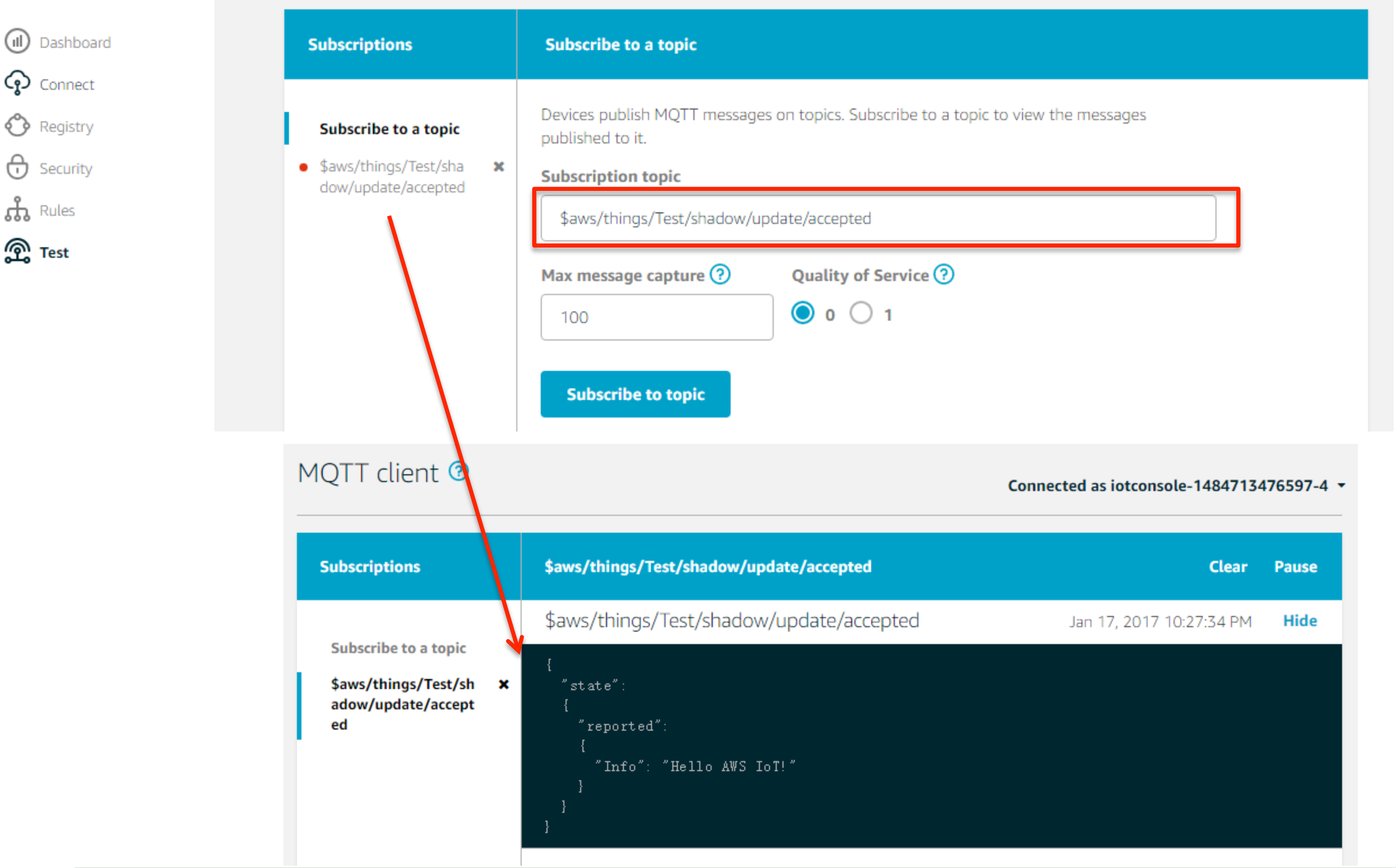
Shadow Document

Last update: Jan 17, 2017 10:24:27 PM -0600

Shadow state:

```
{
  "reported": {
    "Hello": "Hello AWS IoT"
  }
}
```

Basic Interact: Subscribe



Devices publish MQTT messages on topics. Subscribe to a topic to view the messages published to it.

Subscription topic: $aws/things/Test/shadow/update/accepted

Max message capture: 100

Quality of Service: ● 0 ○ 1

Subscriptions: $aws/things/Test/shadow/update/accepted ×

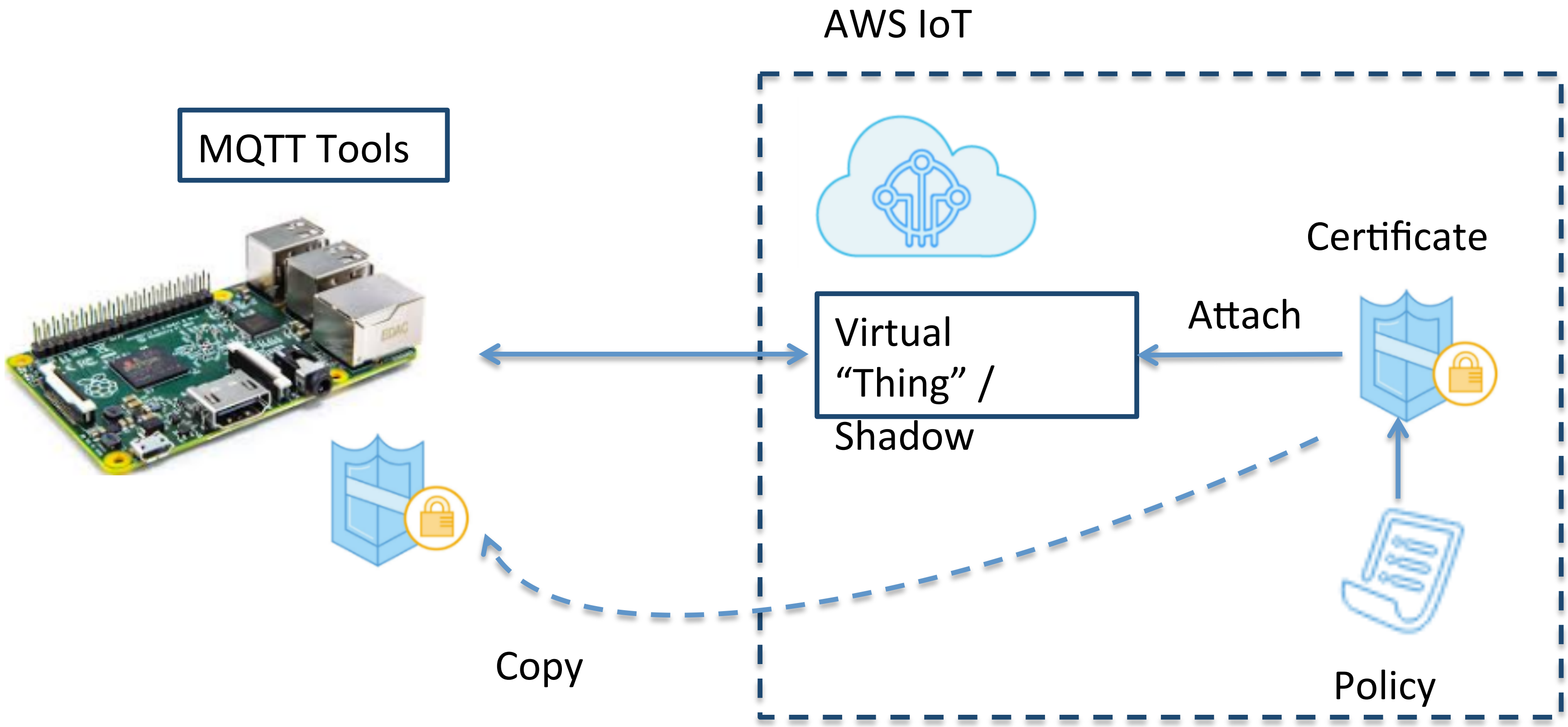
Connected as iotconsole-1484713476597-4

$aws/things/Test/shadow/update/accepted

$aws/things/Test/shadow/update/accepted Jan 17, 2017 10:27:34 PM

```
{
  "state":
  {
    "reported":
    {
      "Info": "Hello AWS IoT!"
    }
  }
}
```

Step 2: Connect a Physical Device



AWS IoT

MQTT Tools

Certificate

Virtual "Thing" / Shadow

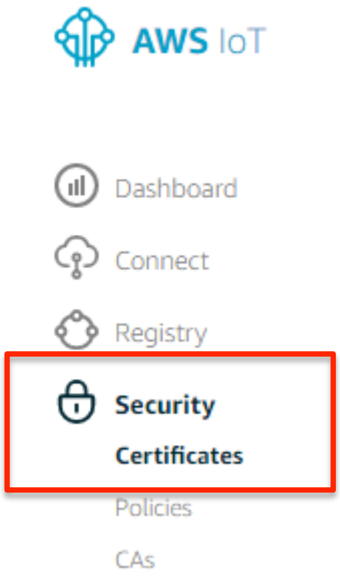
Attach

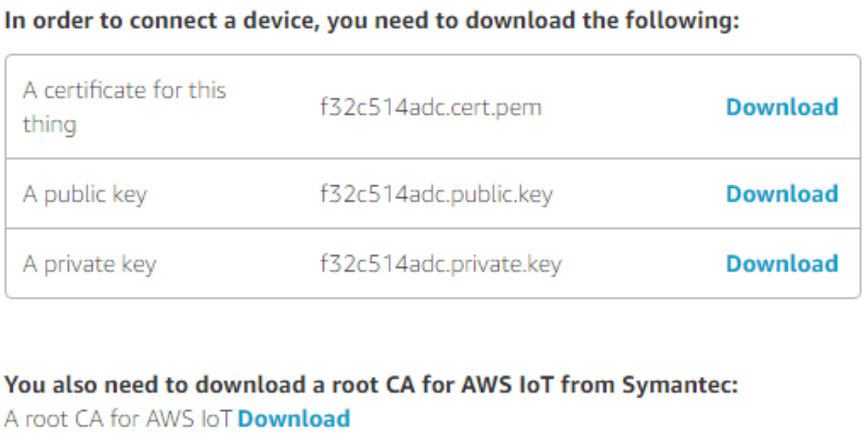
Copy

Policy

Create and get Certificates

- Create Certificates
  - Security → Certificates → Create
- Download Cert Files
  - 1. public & private key
  - 2. thing cert
  - 3. Root CA for AWS





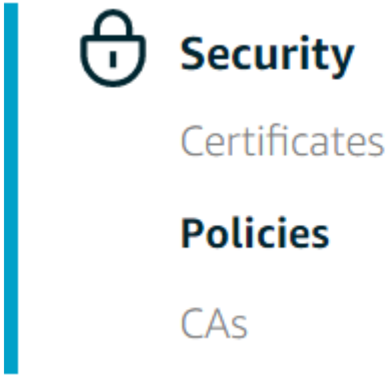
In order to connect a device, you need to download the following:

A certificate for this thing	f32c514adc.cert.pem	Download
A public key	f32c514adc.public.key	Download
A private key	f32c514adc.private.key	Download

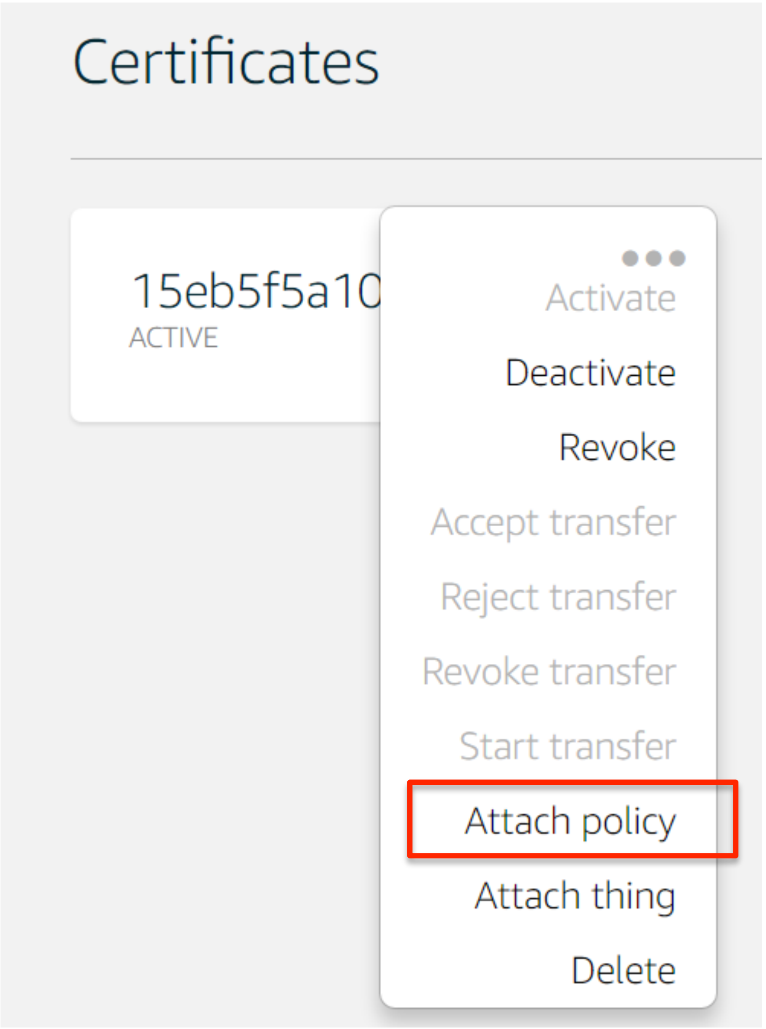
You also need to download a root CA for AWS IoT from Symantec:
A root CA for AWS IoT **Download**

Create Policy and attach it to cert

- Create Policy



- Attach Policy to Certificates

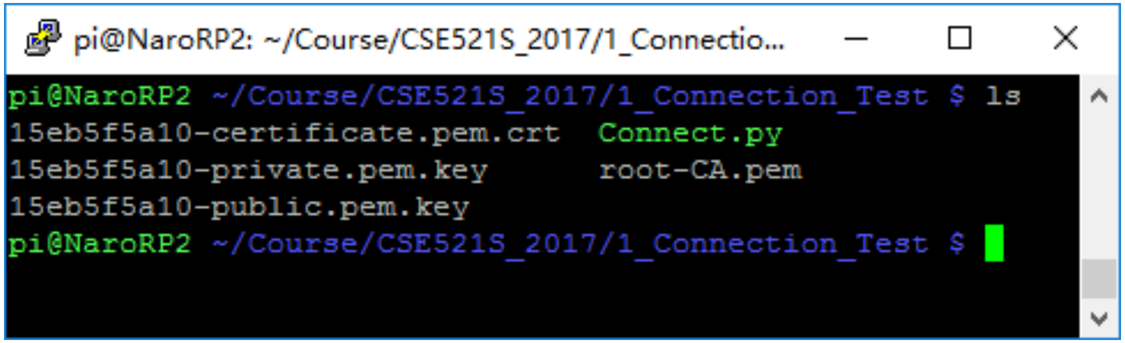


Connect your Device

- Copy certificates to RP2
- Choose your AWS SDK (support MQTT)
  - ❑ Node JS
  - ❑ Python
  - ❑ Java
  - ❑ Embedded C
- You can also use third party MQTT tools
  - ❑ Python (paho mqtt library)

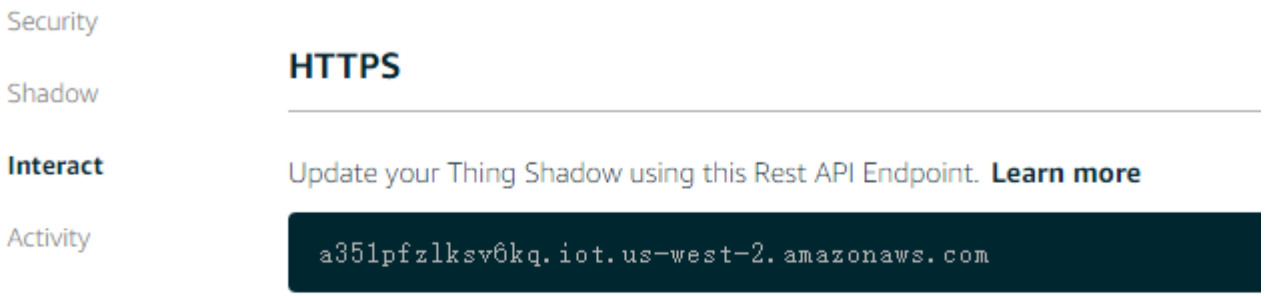
Some Notes

- 1. You will need these certification when setting up the TLS1.2 verification



```
pi@NaroRP2 ~/Course/CSE521S_2017/1_Connection_Test $ ls
15eb5f5a10-certificate.pem.crt  Connect.py
15eb5f5a10-private.pem.key      root-CA.pem
15eb5f5a10-public.pem.key
pi@NaroRP2 ~/Course/CSE521S_2017/1_Connection_Test $
```

- 2. You will need the endpoint and port (8883) when connect to AWS IoT Gateway



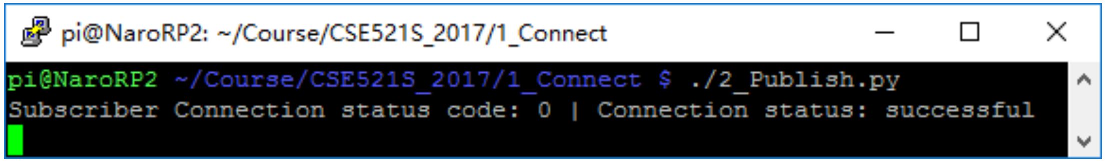
HTTPS

Update your Thing Shadow using this Rest API Endpoint.

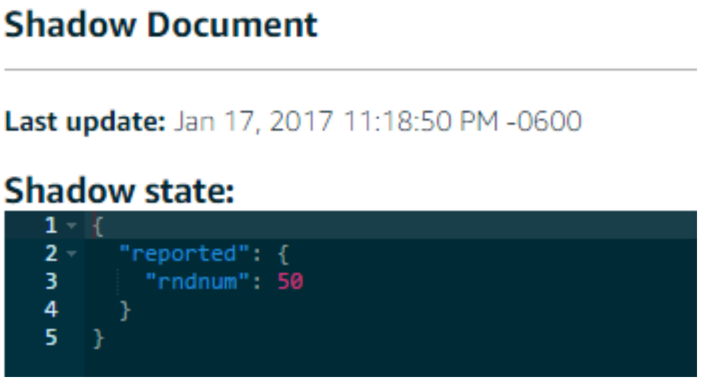
```
a351pfzlksv6kq.iot.us-west-2.amazonaws.com
```

Publish / Subscribe

- ➢ Publish
- ➢ payload = "{\"state\":{\"reported\":{\"rndnum\":**50**}}}"


pi@NaroRP2: ~/Course/CSE521S_2017/1_Connect

```
pi@NaroRP2 ~/Course/CSE521S_2017/1_Connect $ ./2_Publish.py
Subscriber Connection status code: 0 | Connection status: successful
```

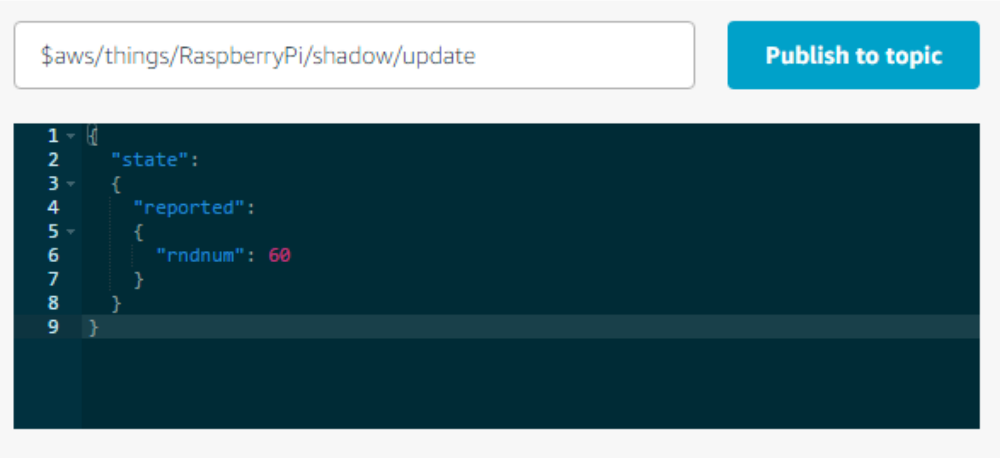

Shadow Document

Last update: Jan 17, 2017 11:18:50 PM -0600

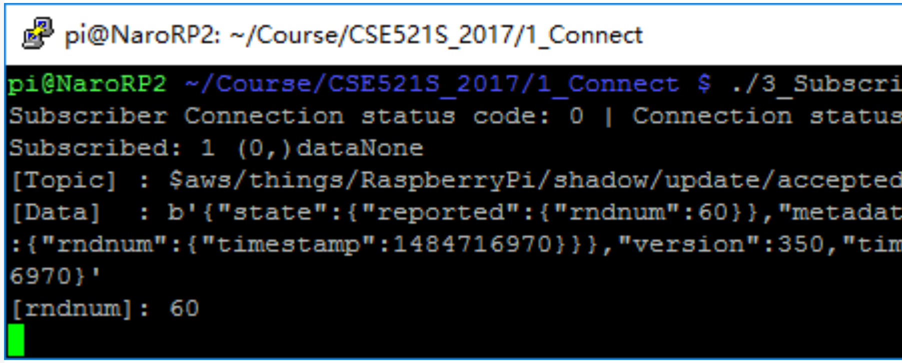
Shadow state:

```
{
  "reported": {
    "rndnum": 50
  }
}
```

- ➢ Subscribe

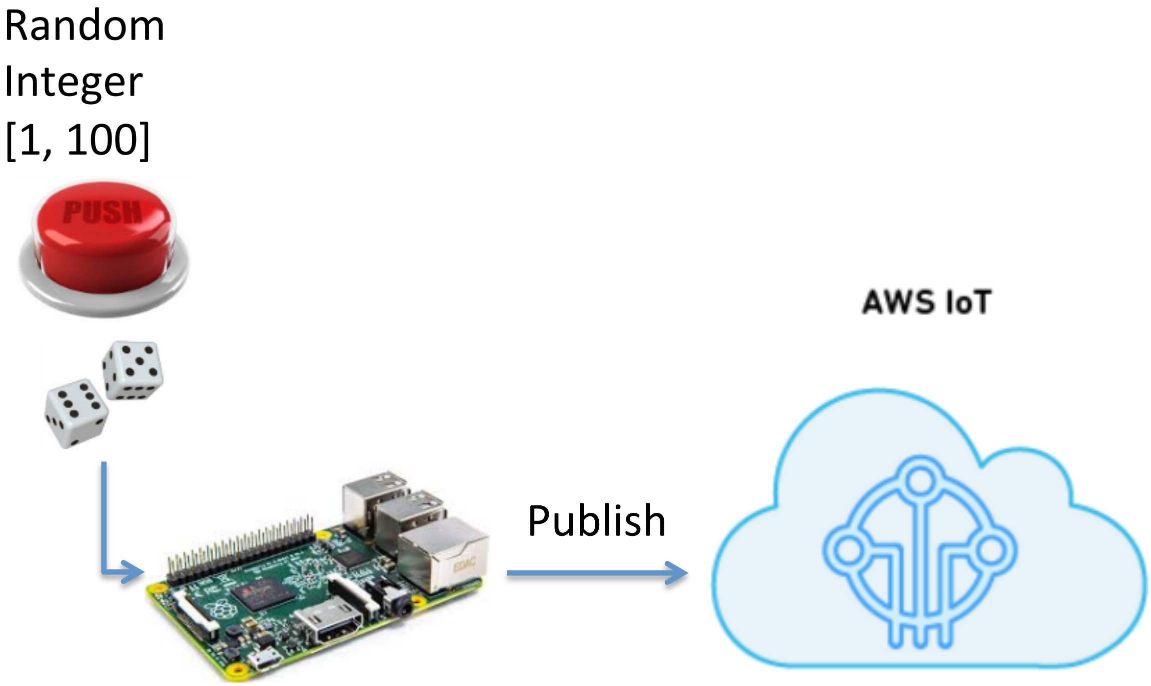

$aws/things/RaspberryPi/shadow/update

```
{
  "state":
  {
    "reported":
    {
      "rndnum": 60
    }
  }
}
```


pi@NaroRP2: ~/Course/CSE521S_2017/1_Connect

```
pi@NaroRP2 ~/Course/CSE521S_2017/1_Connect $ ./3_Subscri
Subscriber Connection status code: 0 | Connection status
Subscribed: 1 (0,)dataNone
[Topic] : $aws/things/RaspberryPi/shadow/update/accepted
[Data]  : b'{"state":{"reported":{"rndnum":60}},"metadat
:{"rndnum":{"timestamp":1484716970}},"version":350,"tim
6970}'
[rndnum]: 60
```

Step 3: Push Button and Publish

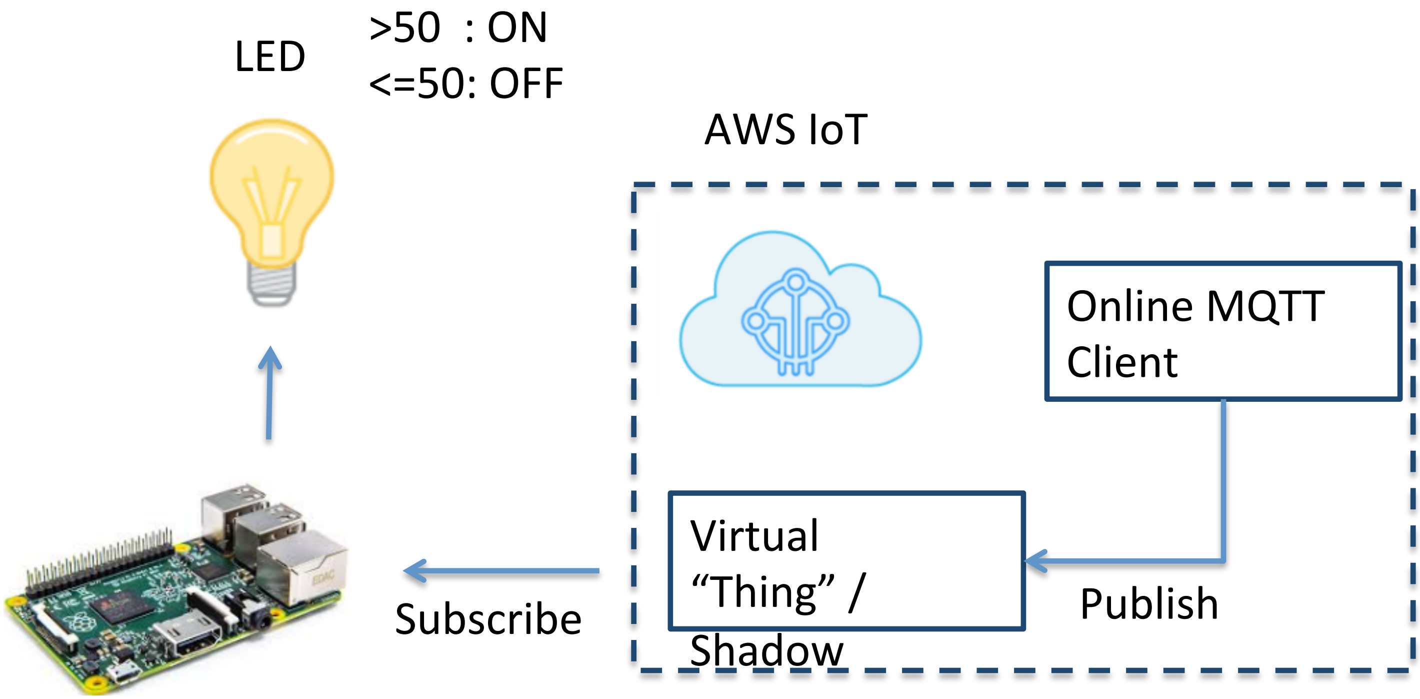


Random
Integer
[1, 100]

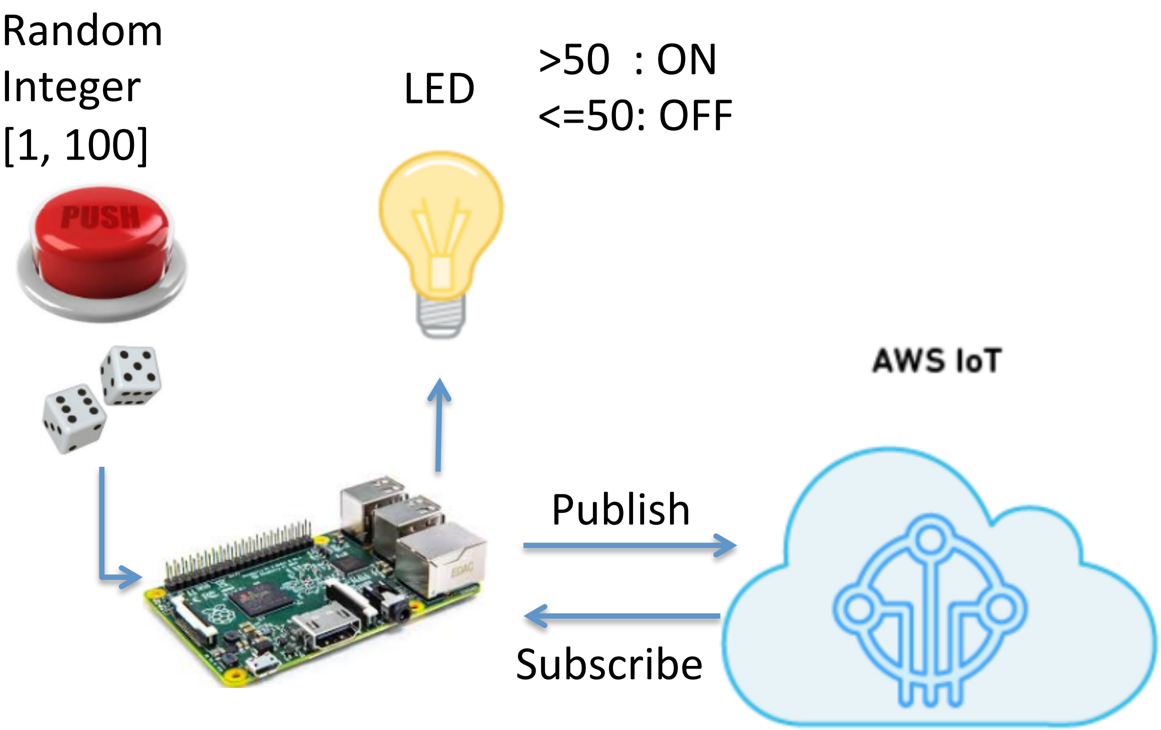
Publish

AWS IoT

Step 4: Subscribe and Lit up LED



Step 5: Combine Them Together



Random Integer [1, 100]

LED

>50 : ON
<=50: OFF

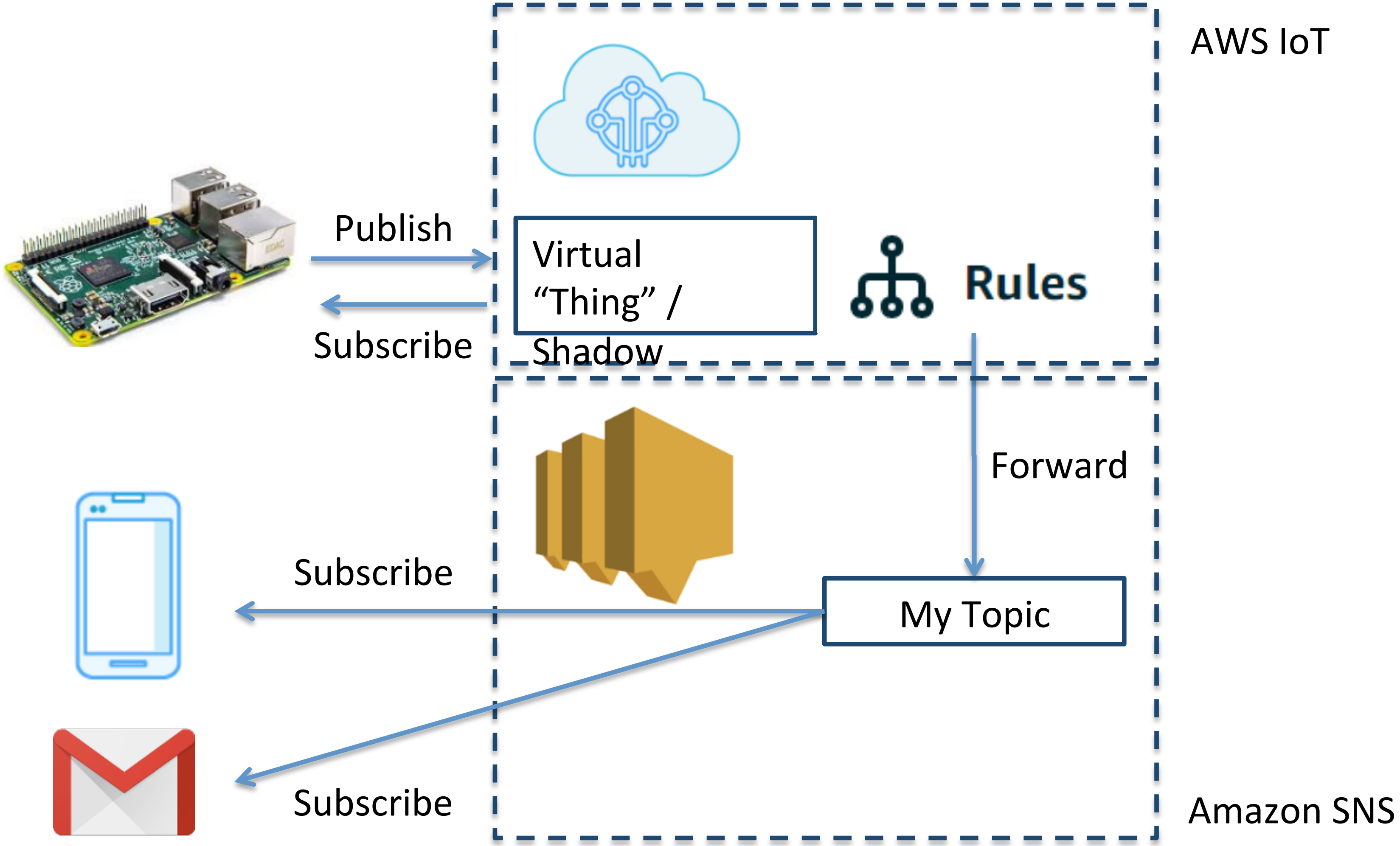
AWS IoT

Publish

Subscribe

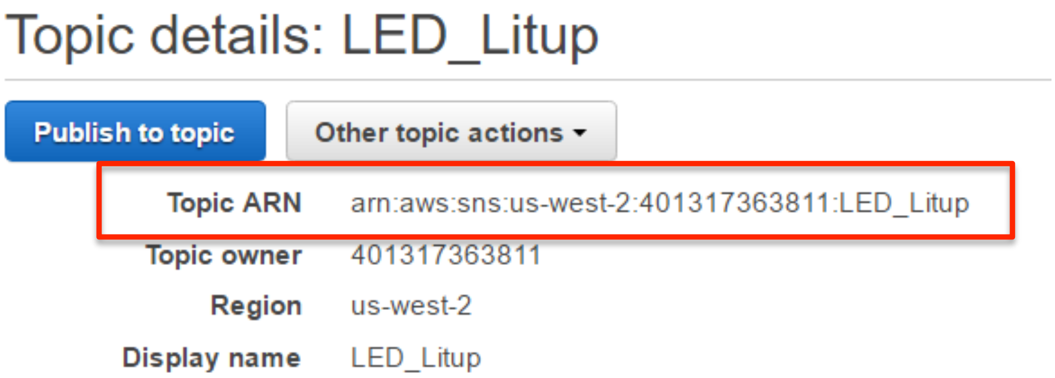
More Fancy: SNS services

- Simple Notification Service



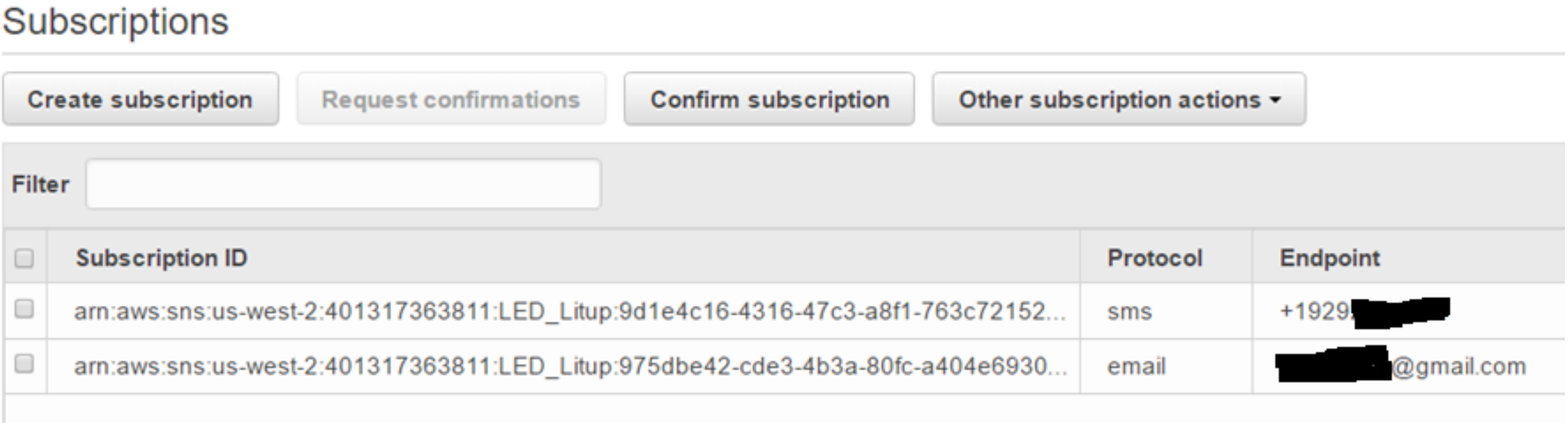
Amazon SNS

- ➢ Create a Topic
  - ❑ ARN will be used later



Topic details: LED_Litup

Topic ARN	arn:aws:sns:us-west-2:401317363811:LED_Litup
Topic owner	401317363811
Region	us-west-2
Display name	LED_Litup

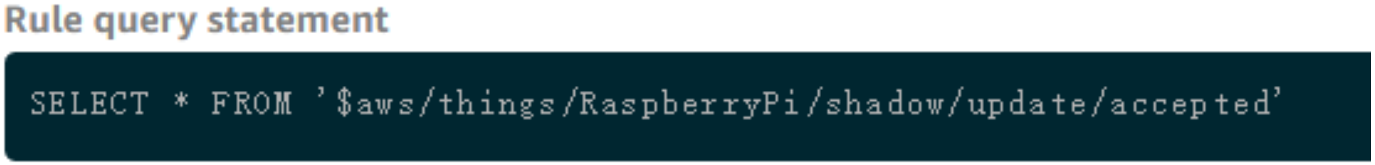


Subscriptions

□	Subscription ID	Protocol	Endpoint
□	arn:aws:sns:us-west-2:401317363811:LED_Litup:9d1e4c16-4316-47c3-a8f1-763c72152...	sms	+1929[redacted]
□	arn:aws:sns:us-west-2:401317363811:LED_Litup:975dbe42-cde3-4b3a-80fc-a404e6930...	email	[redacted]@gmail.com

Create a Rule in Amazon IoT

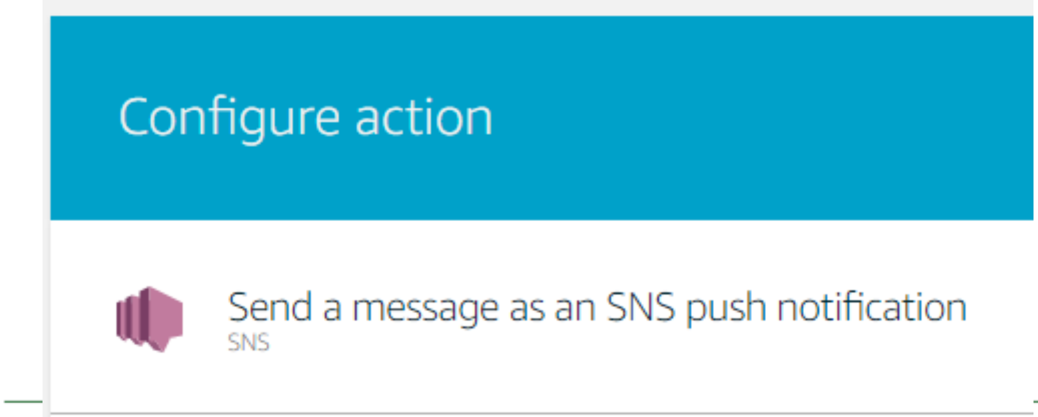
- Add a query to filter your inteseting topic (event)



Rule query statement

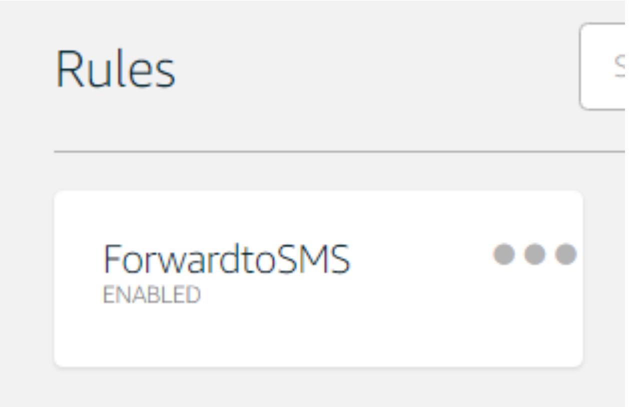
```
SELECT * FROM ’$aws/things/RaspberryPi/shadow/update/accepted’
```

- Add an Action:
  - ❑ Forward this message to SNS
  - ❑ Specify Dest ARN
  - ❑ Enable Rule



Configure action

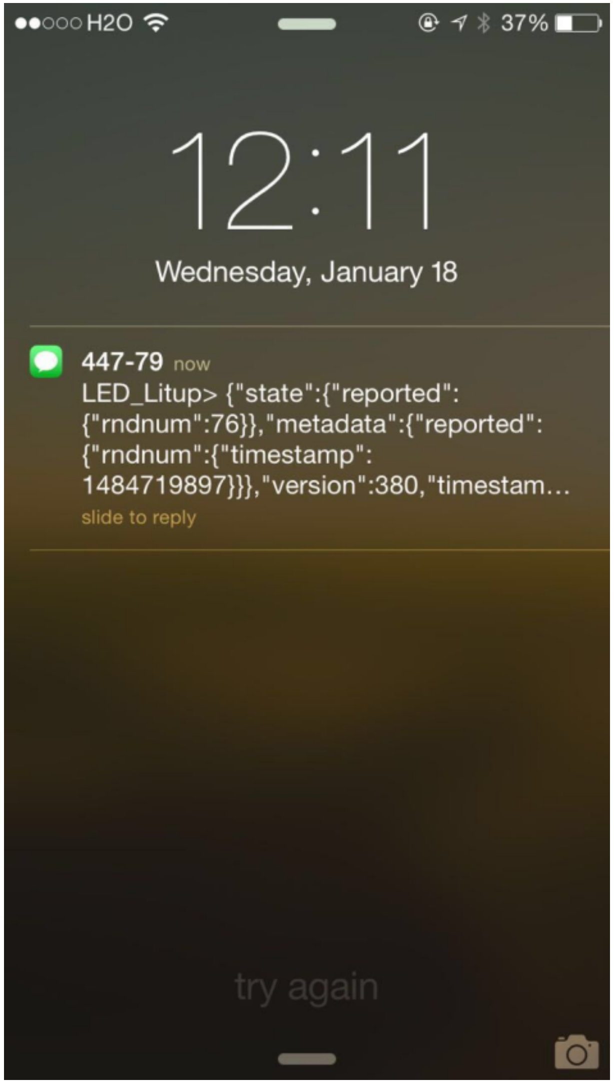
Send a message as an SNS push notification
SNS



Rules

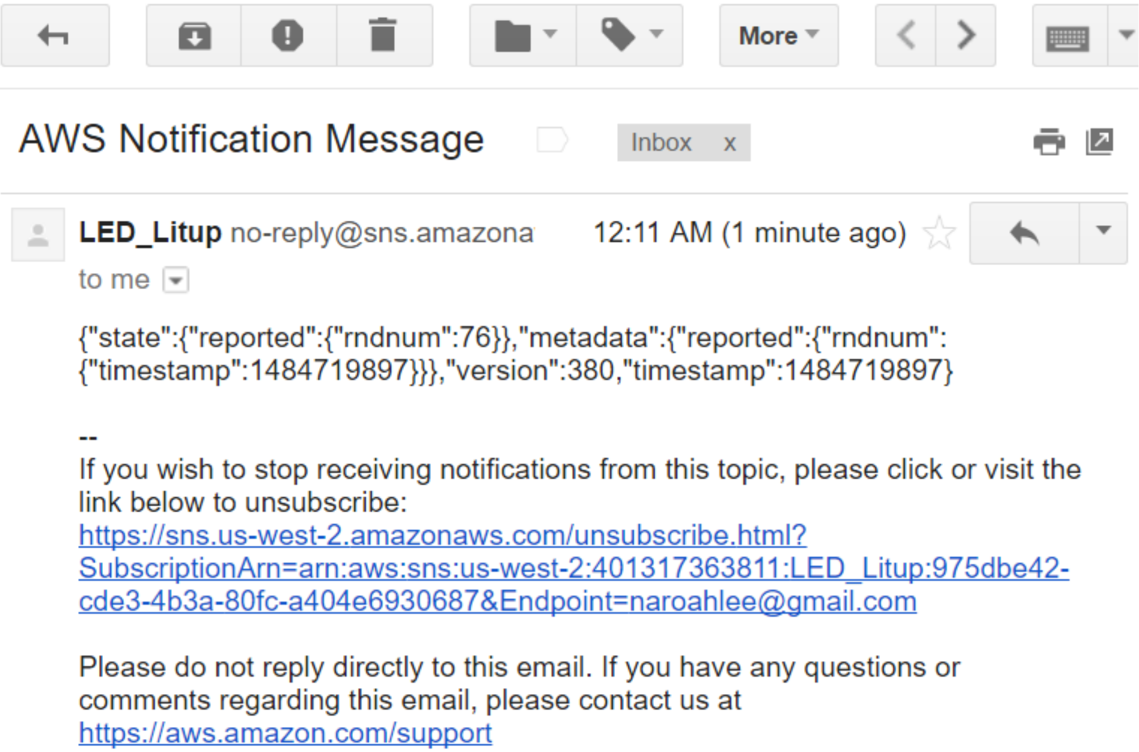
ForwardtoSMS
ENABLED

Notification on SMS & Email



447-79 now

LED_Litup> {"state":{"reported":{"rndnum":76}},"metadata":{"reported":{"rndnum":{"timestamp":1484719897}}},"version":380,"timestam…



AWS Notification Message

LED_Litup no-reply@sns.amazona 12:11 AM (1 minute ago)

to me

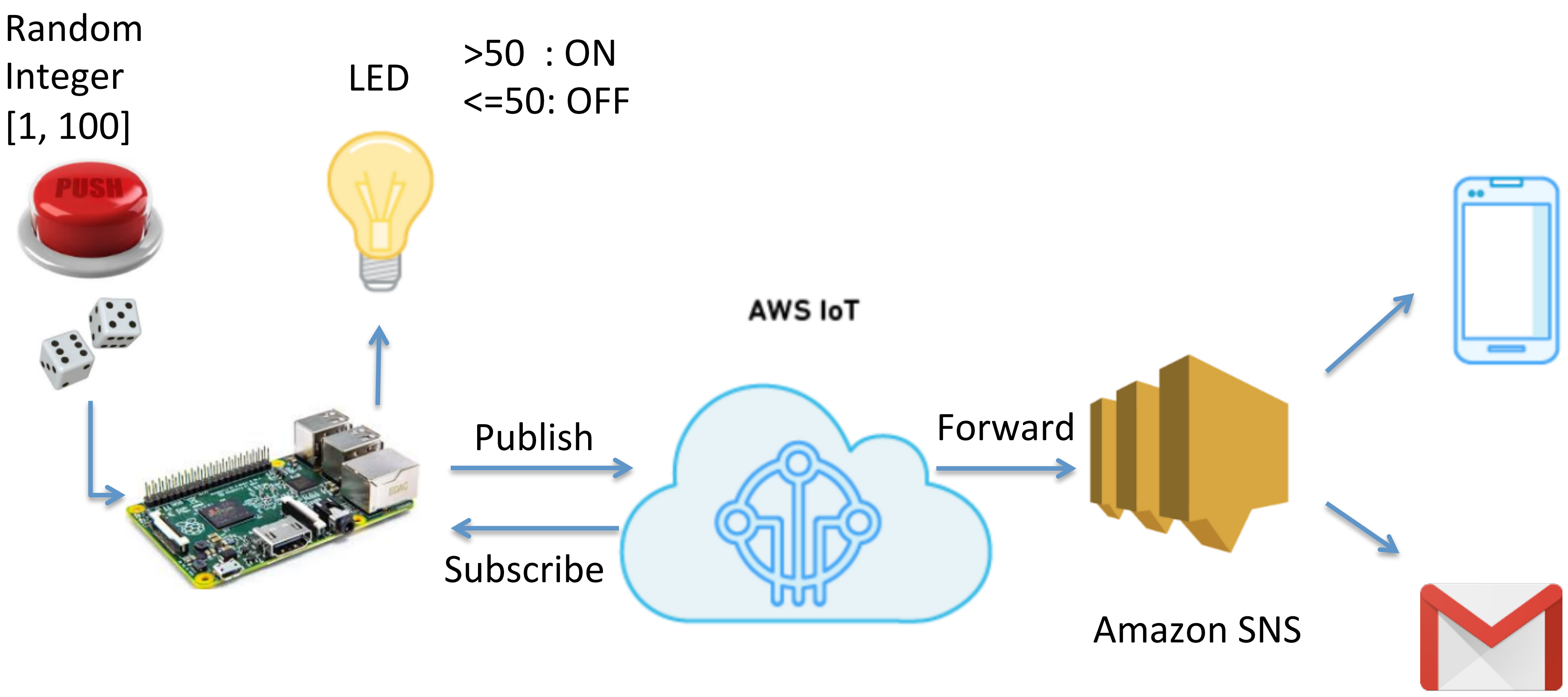
{"state":{"reported":{"rndnum":76}},"metadata":{"reported":{"rndnum":{"timestamp":1484719897}}},"version":380,"timestamp":1484719897}

--

If you wish to stop receiving notifications from this topic, please click or visit the link below to unsubscribe:
https://sns.us-west-2.amazonaws.com/unsubscribe.html?SubscriptionArn=arn:aws:sns:us-west-2:401317363811:LED_Litup:975dbe42-cde3-4b3a-80fc-a404e6930687&Endpoint=naroahlee@gmail.com

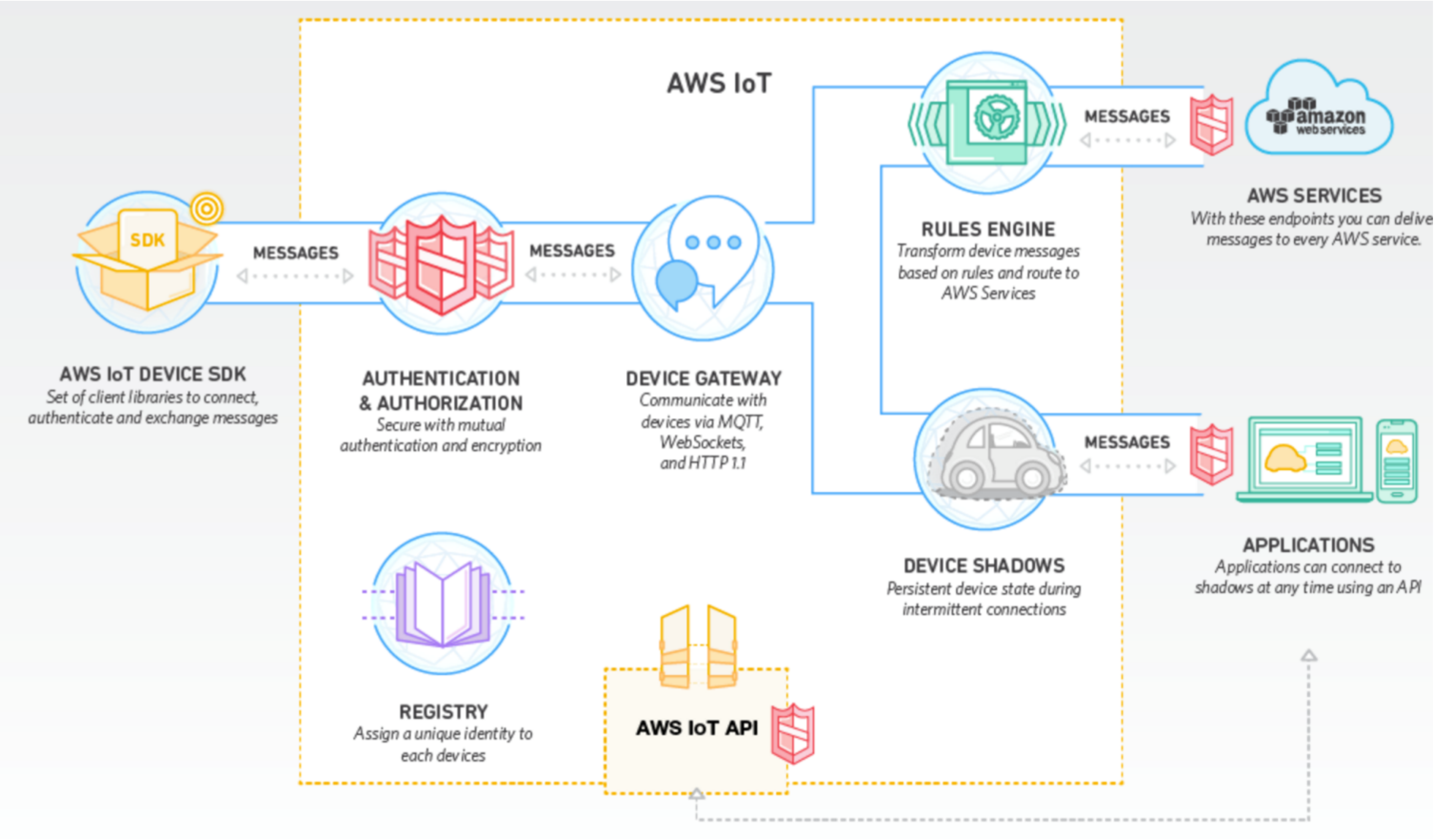
Please do not reply directly to this email. If you have any questions or comments regarding this email, please contact us at https://aws.amazon.com/support

Recap: Hello AWS IoT!



Source: https://aws.amazon.com/iot-platform/

Recap: Amazon IoT Architecture



AWS IoT DEVICE SDK
Set of client libraries to connect, authenticate and exchange messages

AUTHENTICATION & AUTHORIZATION
Secure with mutual authentication and encryption

DEVICE GATEWAY
Communicate with devices via MQTT, WebSockets, and HTTP 1.1

RULES ENGINE
Transform device messages based on rules and route to AWS Services

AWS SERVICES
With these endpoints you can delive messages to every AWS service.

DEVICE SHADOWS
Persistent device state during intermittent connections

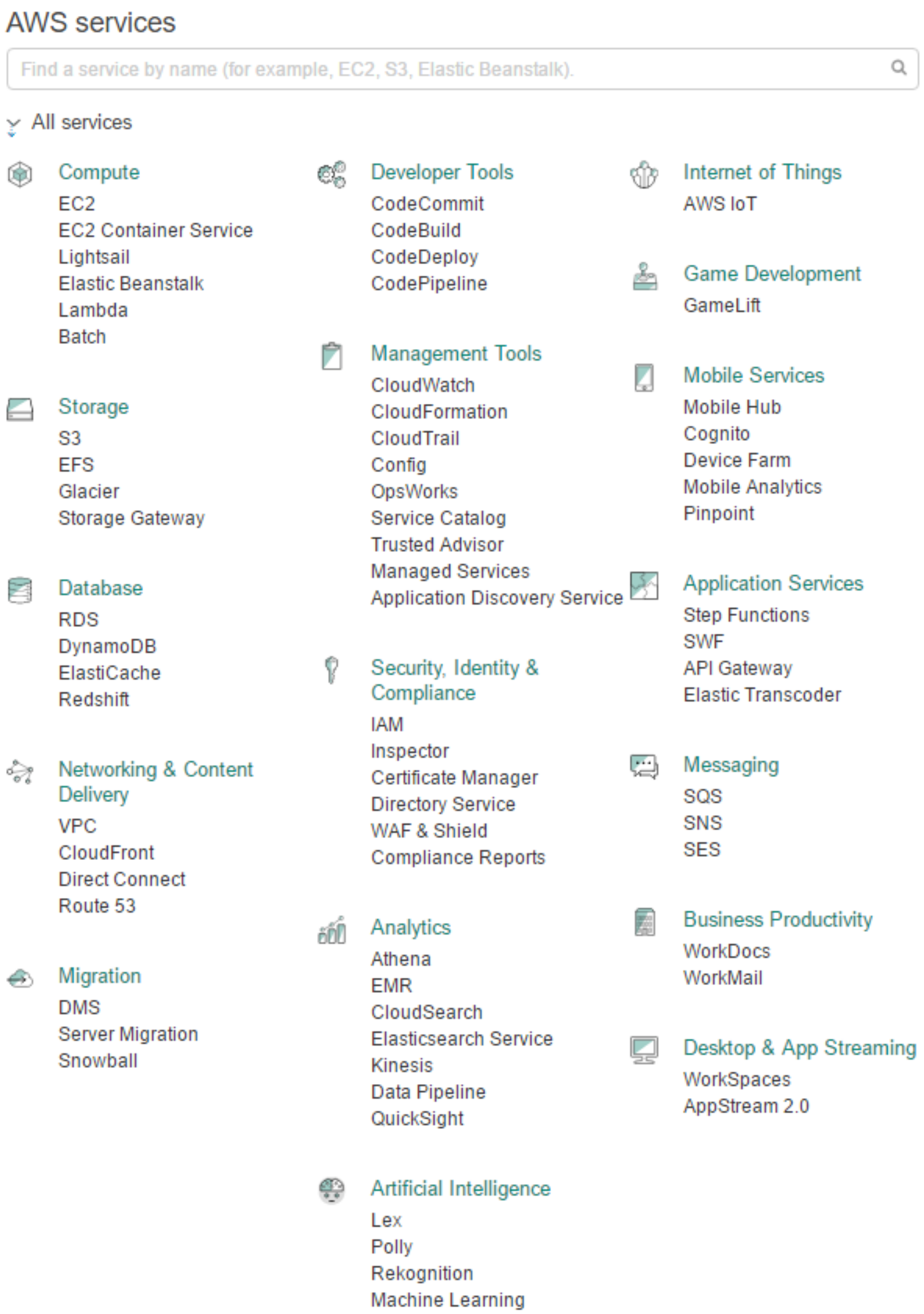
APPLICATIONS
Applications can connect to shadows at any time using an API

REGISTRY
Assign a unique identity to each devices

AWS IoT API

Be Creative!

- Bunch of Services
- **Embedded systems + Cloud Services…**
- IoT!



AWS services

Find a service by name (for example, EC2, S3, Elastic Beanstalk).

All services

Compute
EC2
EC2 Container Service
Lightsail
Elastic Beanstalk
Lambda
Batch

Storage
S3
EFS
Glacier
Storage Gateway

Database
RDS
DynamoDB
ElastiCache
Redshift

Networking & Content Delivery
VPC
CloudFront
Direct Connect
Route 53

Migration
DMS
Server Migration
Snowball

Developer Tools
CodeCommit
CodeBuild
CodeDeploy
CodePipeline

Management Tools
CloudWatch
CloudFormation
CloudTrail
Config
OpsWorks
Service Catalog
Trusted Advisor
Managed Services
Application Discovery Service

Security, Identity & Compliance
IAM
Inspector
Certificate Manager
Directory Service
WAF & Shield
Compliance Reports

Analytics
Athena
EMR
CloudSearch
Elasticsearch Service
Kinesis
Data Pipeline
QuickSight

Artificial Intelligence
Lex
Polly
Rekognition
Machine Learning

Internet of Things
AWS IoT

Game Development
GameLift

Mobile Services
Mobile Hub
Cognito
Device Farm
Mobile Analytics
Pinpoint

Application Services
Step Functions
SWF
API Gateway
Elastic Transcoder

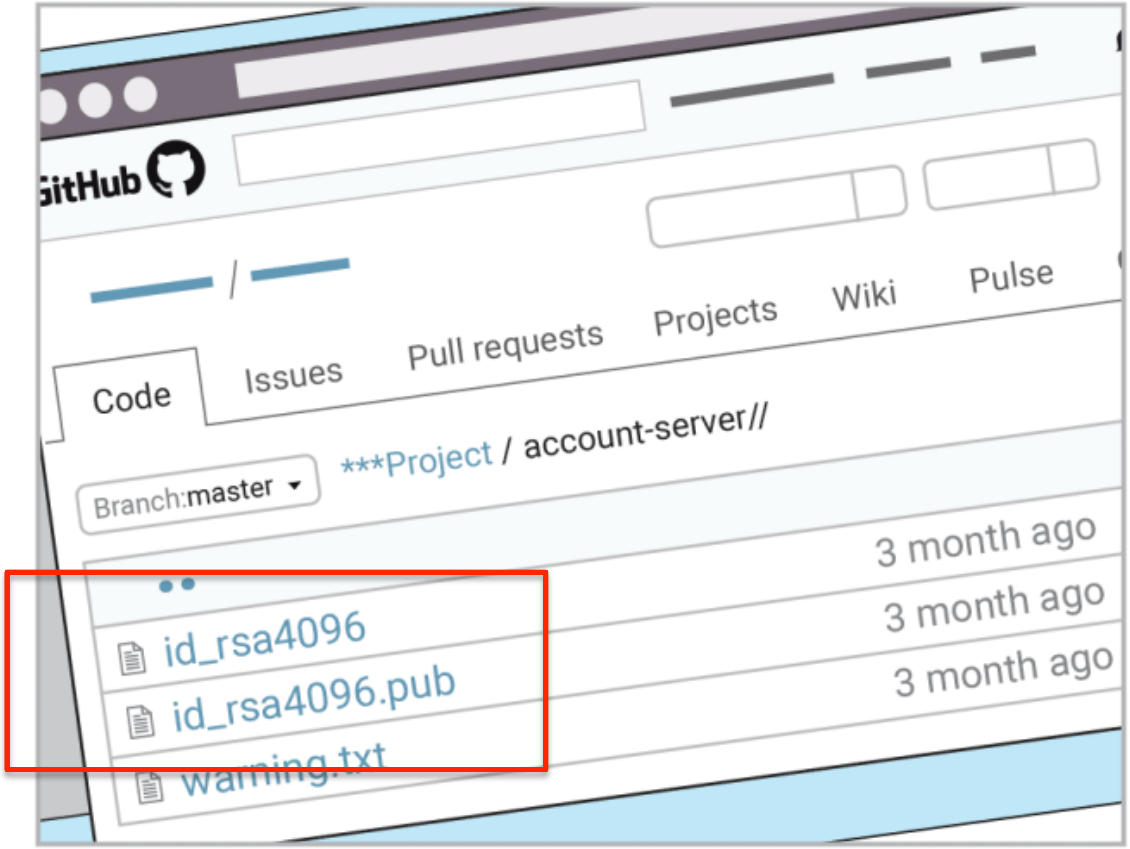
Messaging
SQS
SNS
SES

Business Productivity
WorkDocs
WorkMail

Desktop & App Streaming
WorkSpaces
AppStream 2.0

One More Thing: Security

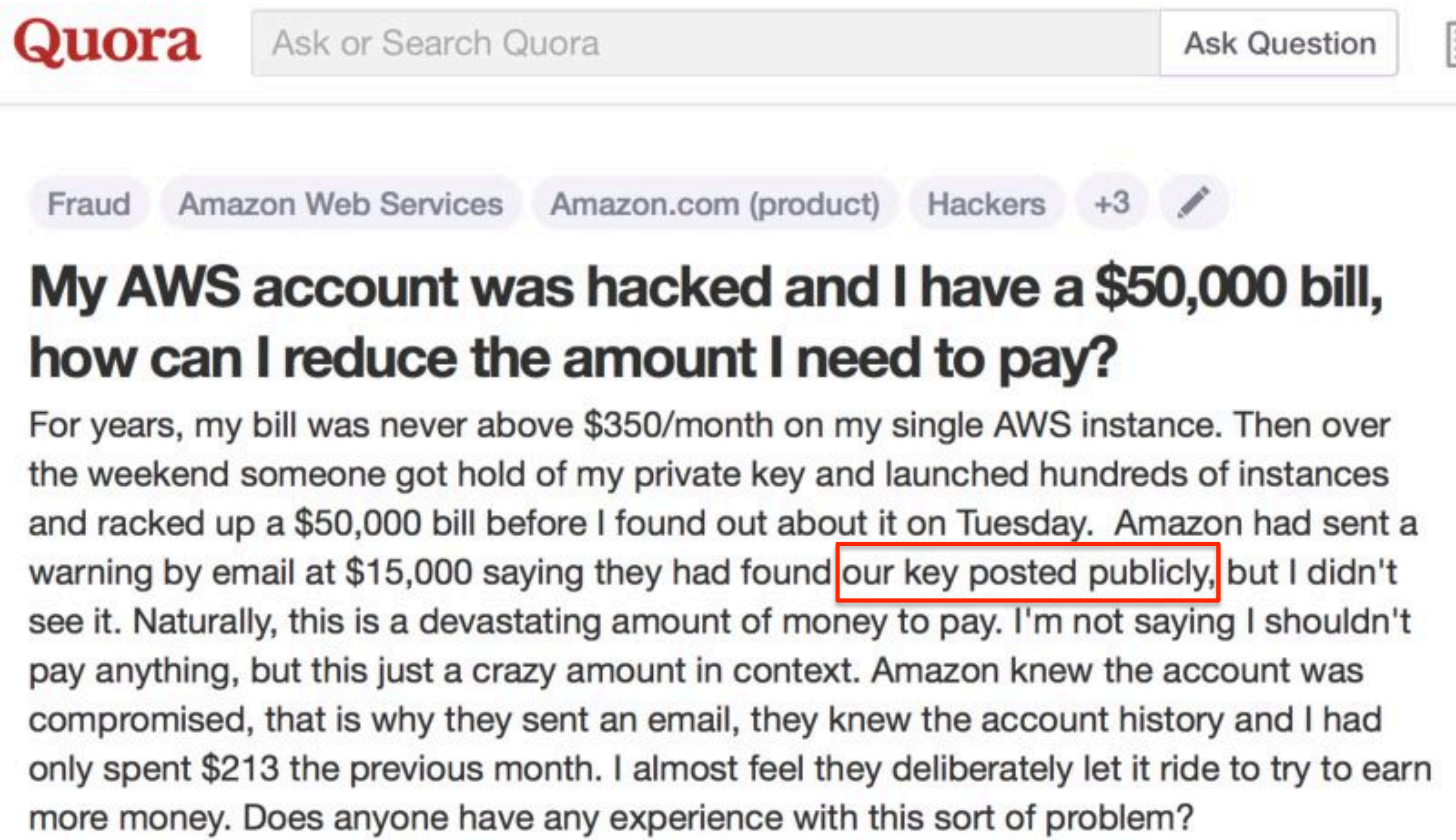
- DON'T UPLOAD YOUR PUBLIC KEY!!!



Source: WeChat Subscriptions: 西乔《神秘的程序员们 39》 Geek Life Chpt 39.

What if… 50,000 AWS Bill!

CPSL
Cyber-Physical
Systems Laboratory



My AWS account was hacked and I have a $50,000 bill, how can I reduce the amount I need to pay?

For years, my bill was never above $350/month on my single AWS instance. Then over the weekend someone got hold of my private key and launched hundreds of instances and racked up a $50,000 bill before I found out about it on Tuesday. Amazon had sent a warning by email at $15,000 saying they had found our key posted publicly, but I didn't see it. Naturally, this is a devastating amount of money to pay. I'm not saying I shouldn't pay anything, but this just a crazy amount in context. Amazon knew the account was compromised, that is why they sent an email, they knew the account history and I had only spent $213 the previous month. I almost feel they deliberately let it ride to try to earn more money. Does anyone have any experience with this sort of problem?

Source: https://www.quora.com/My-AWS-account-was-hacked-and-I-have-a-50-000-bill-how-can-I-reduce-the-amount-I-need-to-pay

Pointers

- Amazon IoT
  - ❑ http://docs.aws.amazon.com/iot/latest/developerguide/what-is-aws-iot.html
- Amazon SNS
  - ❑ http://docs.aws.amazon.com/sns/latest/dg/welcome.html
- AWS Resource list for course projects
  - ❑ http://cps.cse.wustl.edu/index.php/AWS_Resources
- Apply for $40 credits for Amazon AWS
  - ❑ https://aws.amazon.com/education/awseducate/apply/

Project Requirements

- Run in public cloud
- Difficulty varies for listed candidates - will take difficulty into consideration when grading.
- Will grade based on
  - project difficulty
  - quality and depth of work
  - workload distribution among team members
- Milestones: proposal, demo1, demo2, final demo, report.
- Start early! Discuss with us and Dr. Lu