iSECpartners
part of nccgroup

Demystifying Security in the Cloud

AWS Scout

Jonathan Chittenden

Quick Introduction

iSECpartners
part of nccgroup

NYU:poly

POLYTECHNIC INSTITUTE OF NYU

Agenda

iSECpartners part of nccgroup

- Motivation
- Elastic Compute Cloud (EC2)
- Simple Storage Service (S3)
- Identity Access Management (IAM)

Brief Introduction of EC2

iSECpartners part of nccgroup

- EC2 is an Amazon Web Service that allows users to rent virtual machines.
  - The process is extremely easy:
    - Select an Amazon Machine Image (AMI)
      - E.g. Ubuntu x64
    - Specify some instance details (like what zone or kernel)
    - Select a key pair
    - Place instance in a security group
      - E.g. web-prod

AMI Security Concerns

iSECpartners part of nccgroup

- Sharing your AMI? At a minimum you should:
  - Securely delete credentials, certificates, and key material
- Using a community AMI? Check for:
  - SSH Authorized Keys
  - Active connections to unknown hosts (ncat backdoor, etc)

EC2 Key Pairs

iSECpartners part of nccgroup

- The use of key pairs allow you to securely and remotely connect to your instance.
  - Amazon will help you generate and prompt you to save your private key.
- And what of shared environments?
  - Employee Turnover
  - How do you monitor access?

EC2 Security Groups

iSECpartners part of nccgroup

- User defined access rules that specify what traffic may be delivered to your instance(s).

- Anyone want to take a shot at deciphering the security group below?

```
GROUP    sg-2eac845a    111122223333    WebServers    web
PERMISSION       111122223333    WebServers ALLOWS  tcp      80       80
FROM     CIDR     0.0.0.0/0       ingress
```

Misconfigured Security Groups

iSECpartners part of nccgroup

Security Bulletin

Possible Insecure memcached Configuration

August 10, 2010

Memcached is a popular tool used by many customers to accelerate the delivery of web content. Some recent research has revealed vulnerabilities in memcached that allow attackers to use published exploits for locating interesting servers, extracting information from caches, and inserting data into the caches. Usually this occurs because the servers running memcached are open to the Internet and have exposed the common port 11211/tcp.

The most effective way to avoid exploit is to ensure that none of your memcached servers can be reached via the Internet. They should be placed in dedicated security groups that allow inbound connections only from your web server security group (see this AWS blog post for further information on using security groups to isolate instances and direct traffic). If you're using memcached in production, we recommend auditing your security groups and, if necessary, taking the appropriate steps to prevent direct Internet access to your memcached servers.

- AWS response to SensePost's BlackHat research on Memcached
  http://www.sensepost.com/blog/4873.html

Managing Security Groups

iSECpartners part of nccgroup

- There can be up to 500 security groups.
  - Containing up to 100 rules per group.

- These are then applied to instances…
  - Production, Staging, Development, Management, etc.

Meet The Scout

iSECpartners part of nccgroup

https://github.com/iSECPartners/scout

Image Source: http://youtu.be/geNMzoJ9TEQ

Scout and Security Groups

- Manual Analysis:
  - List-instances: list all instances and their security groups
  - List-groups: list all security groups and their instances

Instance: observer01
Security Group:
rdp

Instance: staging
Security Groups:
jmp-server
staging
rdp

Scout and Security Groups

iSECpartners part of nccgroup

- Automated Analysis:
  - Audit-groups: highlight dangerous ingress permissions
    - Based on **port ratings** provided by user and the **source**.
    - Security Group with port 3389 open to 0.0.0.0/0
  - Compare-groups: compare "known good" with reality

Brief Introduction of S3

iSECpartners part of nccgroup

- Simply put – it's an online storage service
  - Variety of uses

- Access objects through:
  - REST
  - SOAP
  - BitTorrent

S3 Security Functionality

iSECpartners part of nccgroup

- Security features:
  - Access Controls
    - ACLs
    - Bucket Policy
    - IAM Policy
  - Access Logs
  - Encryption
    - Client Side vs Server Side

S3 Access Controls: ACLs

iSECpartners part of nccgroup

- Coarse-grained permission model
  - So either READ, WRITE, READ_ACP, WRITE_ACP, FULL_CONTROL
  - E.g. Grant AllUsers permission to Read to PublicPhotos
- Grantee can be:
  - An AWS Account
  - Predefined Group
    - Authenticated Users
    - All Users
    - Log Delivery

Typical Instagram User

iSECpartners
part of nccgroup

S3 Access Controls: Bucket Policy

iSECpartners part of nccgroup

- Fine-grained permission model

  Grant * permission to **GetObjectTorrent** to **PreviewReleases**, if DateGreaterThan 2012-10-25T15:00:00

  DateLessThan 2012-10-25T16:00:00

- Amazon Policy Generator can be used to assist administrator.
  - Uses their JSON access policy language.

Obligatory Justin Bieber Slide

iSECpartners
part of nccgroup

S3 Access Controls: IAM Policy

iSECpartners part of nccgroup

- Fine
  - C s to it.

Brief Introduction of IAM

iSECpartners part of nccgroup

- Identity Access Management
  - Allows you to create and manage users/groups
  - Allows you to grant access to AWS resources
    - E.g. EC2 or S3
  - Identity Federation

S3 Access Controls: IAM Policy

iSECpartners part of nccgroup

- Fine-grained permission model
  - Create IAM principal and attach IAM policies to it.
    - Create Various Department Groups & Buckets
    - Create IAM Policy for the Specific Buckets
    - Attach the Policies to the Groups

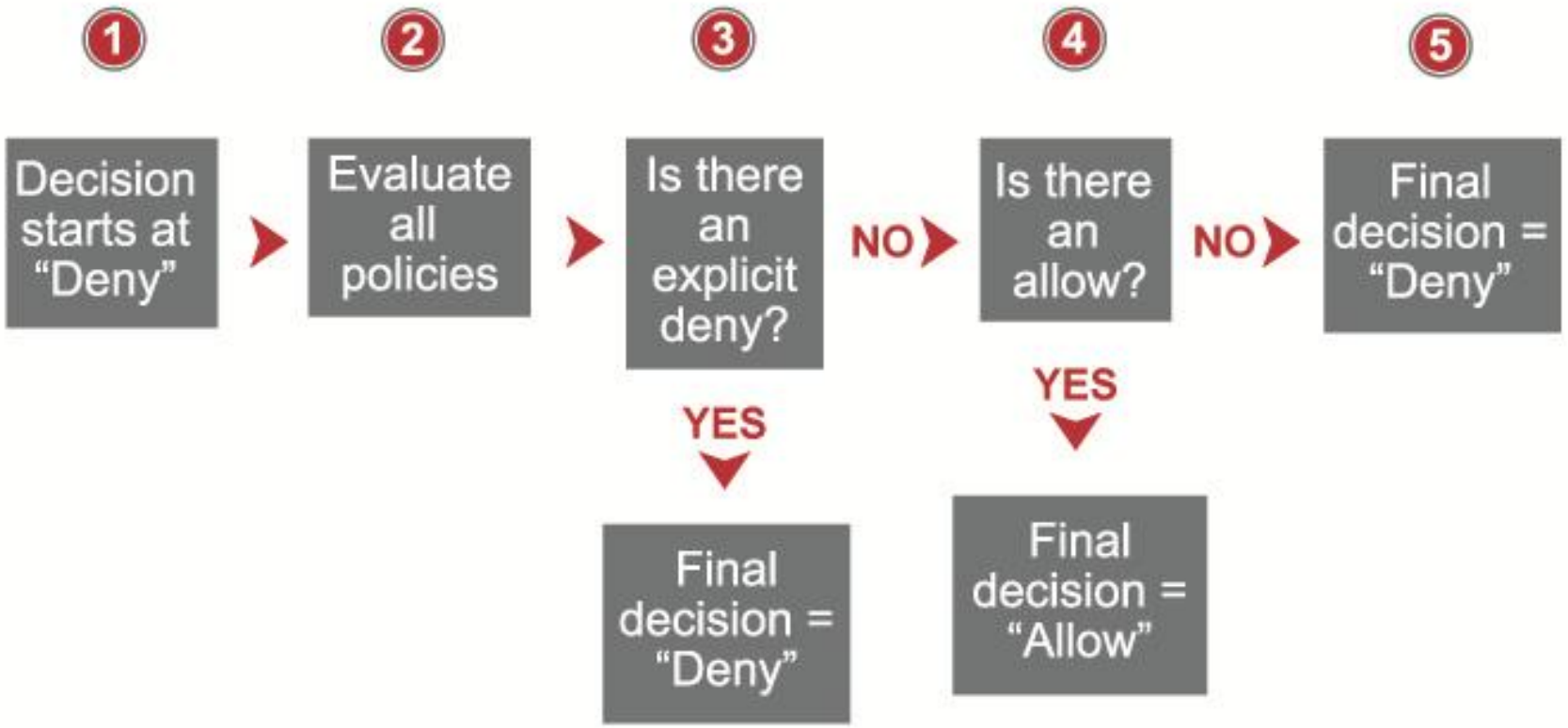
How should they be used?

iSECpartners part of nccgroup

- ACLs
  - Can scale with your application
  - Limited in functionality – simple reads/writes
- Bucket Policy
  - Specific Actions & Conditionals
  - Size Limit of 20kb
- IAM Policy
  - Identity Federation

How does S3 evaluate these?

iSECpartners part of nccgroup



S3: Server Side Encryption

iSECpartners part of nccgroup

- Server Side Encryption
  - Amazon manages keys with AES-256 bit
  - Objects are encrypted, *not* buckets

- Benefits:
  - No need to manage keys
  - Risk transfer

S3: Client Side Encryption

iSECpartners part of nccgroup

- Client Side Encryption
  - You take ownership of managing your keys
  - AWS SDK can make this process very easy
    - Uses Envelope Encryption
- Benefits:
  - More control
  - Master Key compromise simplified

Scout and S3

iSECpartners part of nccgroup

- Access Controls
  - ACLs
    - Costs money to review the ACL for every object/bucket
  - Bucket Policy
  - IAM Policy
    - IAM policies are attached to IAM users – so chances are you are aware of them already.
- Enforcing Encryption

References

iSECpartners part of nccgroup

- Amazon Documentation
  - http://aws.amazon.com/documentation/
- Jeff Jarmoc – "Get Off My Cloud"
  - https://cloudsecurityalliance.org/wp-content/uploads/2012/02/3.Conference-Presentation.Jarmoc.Updated.pdf
- Sense Post – Mining Memcache
  - http://www.sensepost.com/blog/4873.html

Thank You

iSECpartners part of nccgroup

- Jonathan Chittenden
  - Senior Security Consultant at iSEC Partners
  - jonathan@isecpartners.com
  - @loljawn
- Davis Gallinghouse
  - Former Associate Consultant at iSEC Partners
  - @dgalling

Questions?

iSECpartners
part of nccgroup

iSECpartners
part of nccgroup

UK Offices
Manchester - Head Office
Cheltenham
Edinburgh
Leatherhead
London
Thame

European Offices
Amsterdam - Netherlands
Munich – Germany
Zurich - Switzerland

North American Offices
San Francisco
Atlanta
New York
Seattle

Australian Offices
Sydney