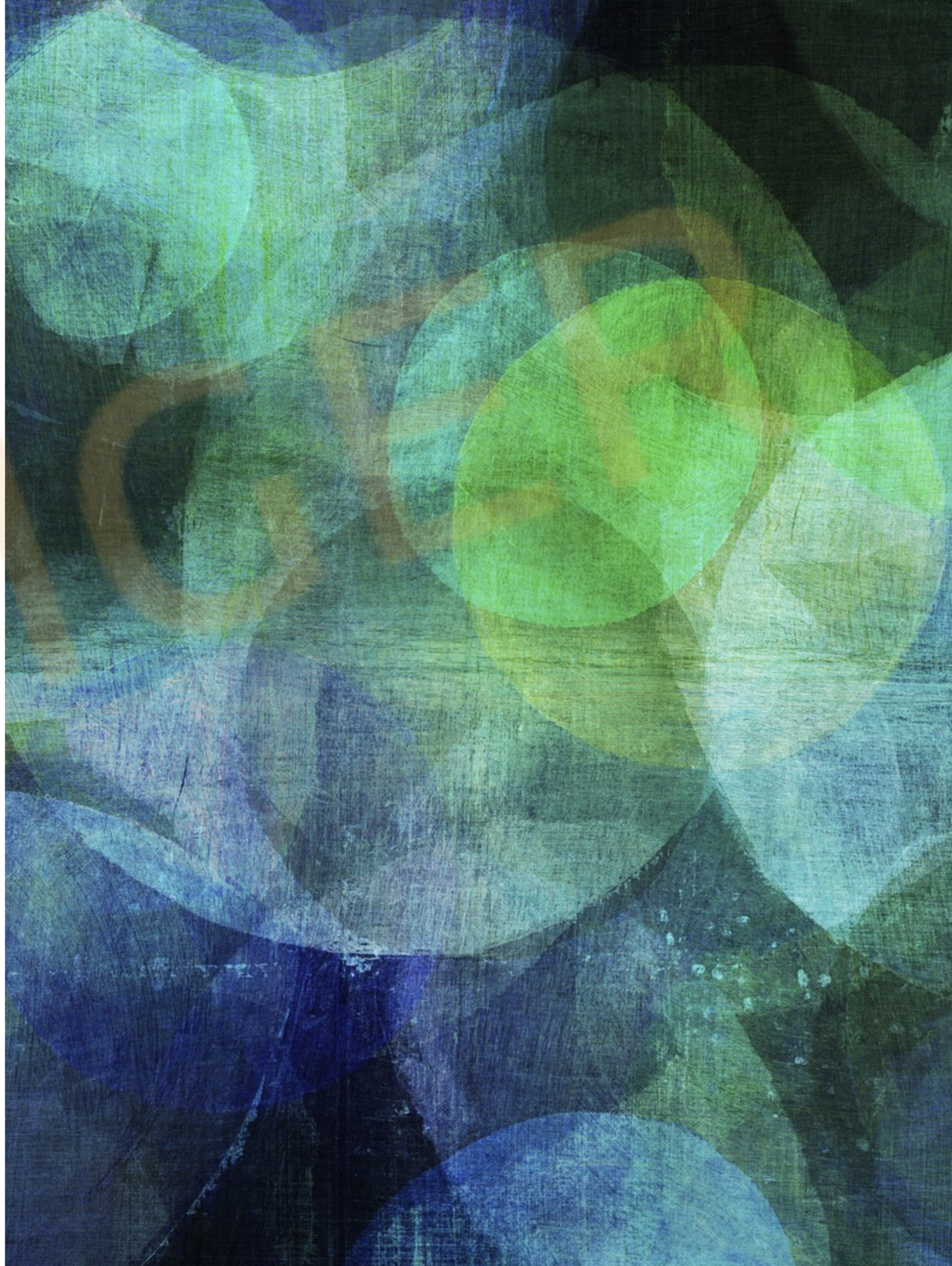
AWS DATA PROCESSING INFRASTRUCTURE 2C

Nan Dun
nan.dun@acm.org



COPYRIGHT POLICY 版权声明

All content included on the Site or third-party platforms as part of the class, such as text, graphics, logos, button icons, images, audio clips, video clips, live streams, digital downloads, data compilations, and software, is the property of BitTiger or its content suppliers and protected by copyright laws.

Any attempt to redistribute or resell BitTiger content will result in the appropriate legal action being taken.

We thank you in advance for respecting our copyrighted content.

For more info see https://www.bittiger.io/termsofuse and https://www.bittiger.io/termsofservice

所有太阁官方网站以及在第三方平台课程中所产生的课程内容，如文本，图形，徽标，按钮图标，图像，音频剪辑，视频剪辑，直播流，数字下载，数据编辑和软件均属于太阁所有并受版权法保护。

对于任何尝试散播或转售BitTiger的所属资料的行为，太阁将采取适当的法律行动。

我们非常感谢您尊重我们的版权内容。

有关详情，请参阅
https://www.bittiger.io/termsofuse
https://www.bittiger.io/termsofservice

DISCLAIMER

I. "All data, information, and opinions expressed in this presentation is for informational purposes only. I do not guarantee the accuracy or reliability of the information provided herein. This is a personal presentation. The opinions expressed here represent my own and not those of my employer."

II. "The copyright of photos, icons, charts, trademarks presented here belong to their authors."

III. "I could be wrong."

OUTLINE

- IAM Policy to limit a user to terminate his/her own instances
- Cross-account bucket copy ACL
- raw2aws.py performance analysis
- Security group rules evaluation

EC2 PROFILE TO PREVENT USER TO STOP OTHER INSTANCES

```
{
    {
        "Effect": "Allow",
        "Action": [
            "ec2:StopInstances",
            "ec2:RebootInstances",
            "ec2:TerminateInstances"
        ],
        "Resource": [
            "arn:aws:ec2:us-west-2:*:instance/*"
        ],
        "Condition": {
            "StringEquals": {
                "ec2:ResourceTag/User": "${aws:username}"
            }
        }
    }
}
```

```
{
    {
        "Effect": "Deny",
        "Action": [
            "ec2:StopInstances",
            "ec2:RebootInstances",
            "ec2:TerminateInstances"
        ],
        "Resource": [
            "arn:aws:ec2:us-west-2:*:instance/*"
        ],
        "Condition": {
            "StringNotEquals": {
                "ec2:ResourceTag/User": "${aws:username}"
            }
        }
    }
}
```

CROSS-ACCOUNT COPY

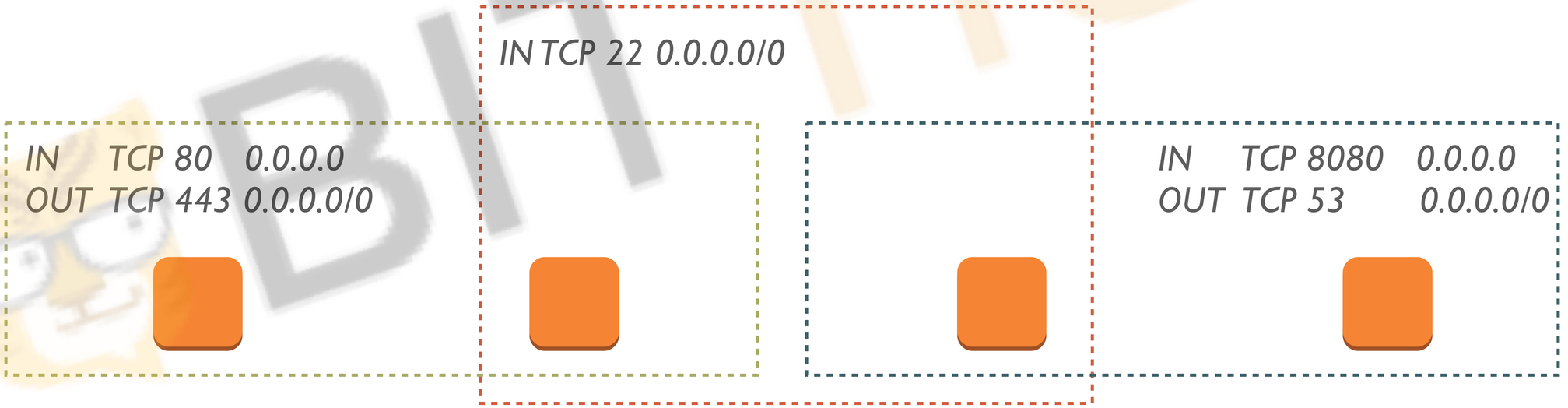
- Access Control List
  - To do a cross-account copy, not only copying, but also grant access to the copied objects
    - http://docs.aws.amazon.com/AmazonS3/latest/dev/acl-overview.html
  - CLI
    - $ aws s3 cp s3://src-bucket s3://dst-bucket --recursive -- acl bucket-owner-full-control
  - Boto3 S3
    - s3 = boto3.resource('s3')
      object = s3.Object('bucket_name','key')
      object.upload_fileobj(content)
      object.Acl().put(ACL='bucket-owner-full-control')
  - S3 bug: multipart_upload does not support ACL
    - https://github.com/aws/aws-cli/issues/1674

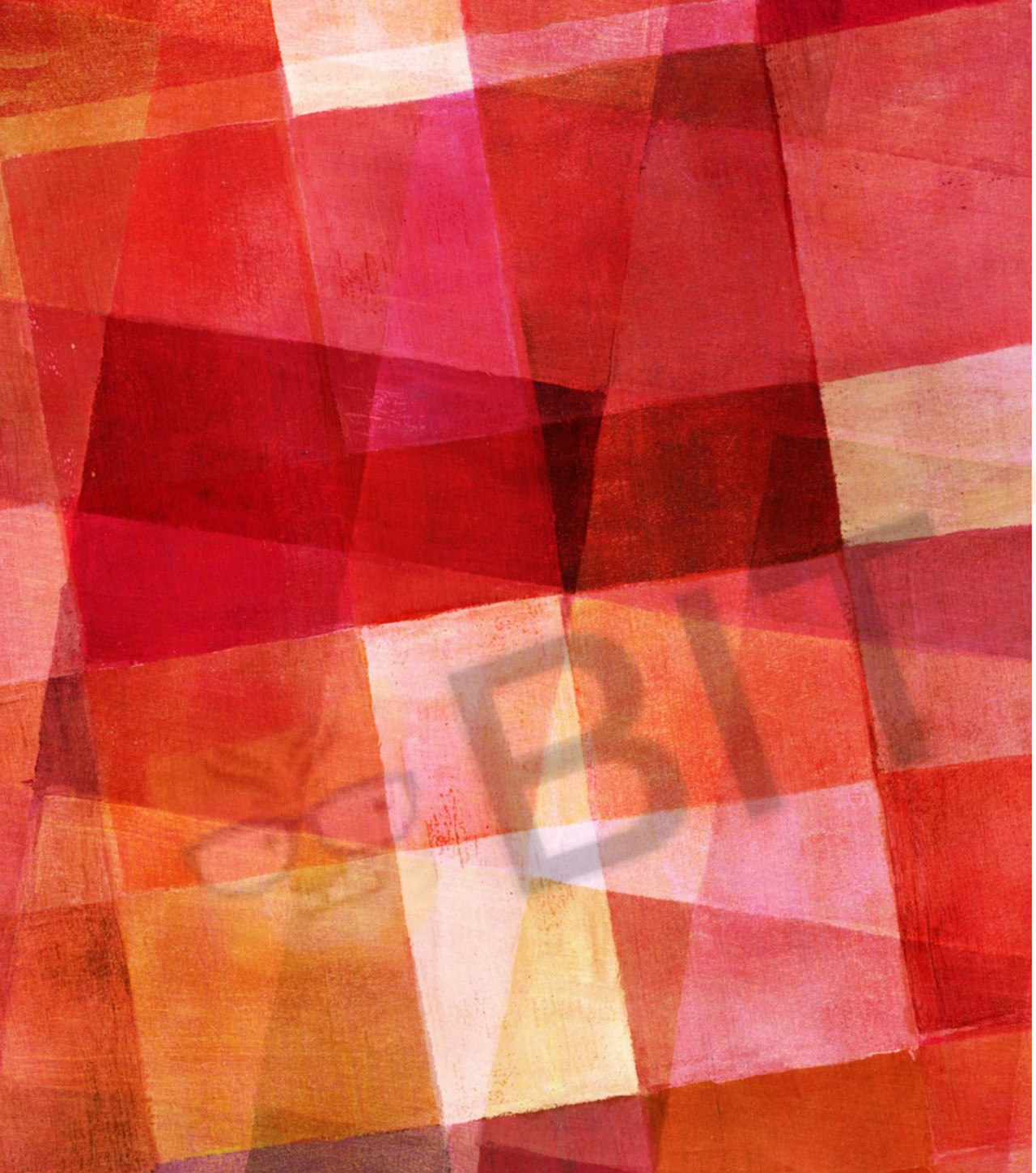
RAW2AWS PERFORMANCE

- 3600 line per second per core
  - Inbound bandwidth: 3600x160 bytes = 562 KB/sec
  - Outbound bandwidth: 3600 x 80 bytes = 281 KB/sec
- Compute-intensive or I/O intensive?
  - c4.8xlarge: 18 concurrent process
    - 10 Gbps > 562 KB/sec x 8 (79 Mbps)
  - CPU is dominate
- More cores per instance or more instances?

SECURITY GROUP RULES

- Whitelist for Inbound/Outbound
  - Default is deny all
  - If there is an allow for the security group which EC2 instances belong to, then allow rule applies





QUESTIONS

- bittiger-aws@googlegroups.com