INSIDE OUT
THE CLOUD HAS NEVER BEEN SO CLOSE

Igal Gofman
Yaron Shani

DID WE LEARN ANYTHING FROM THE RECENT CAPITAL ONE INCIDENT?

HOW SAFE IS YOUR CLOUD ENVIRONMENT?

HOW MUCH YOU INVEST TO MAKE IT SAFE!

CAN YOU ANSWER

- **Who can access what?**
- What resources controlled by which users?
- How many credentials stored on user workstations and servers?
- Who can manage your virtual machines?
- Who can access your cloud data stores?

Did we forget the principle of least privilege (PoLP)?

"Every program and every privileged user of the system should operate using the least amount of privilege necessary to complete the job."

Jerome Saltzer

IN THIS TALK

PUBLIC API ACCESS
Public APIs available from anywhere

ATTACK USE CASES
The risks associated with IAM

GRAPHS TO THE RESCUE!
Using graph to illustrate resource-based attack vectors

DEMO
Risk oriented queries & Algorithms

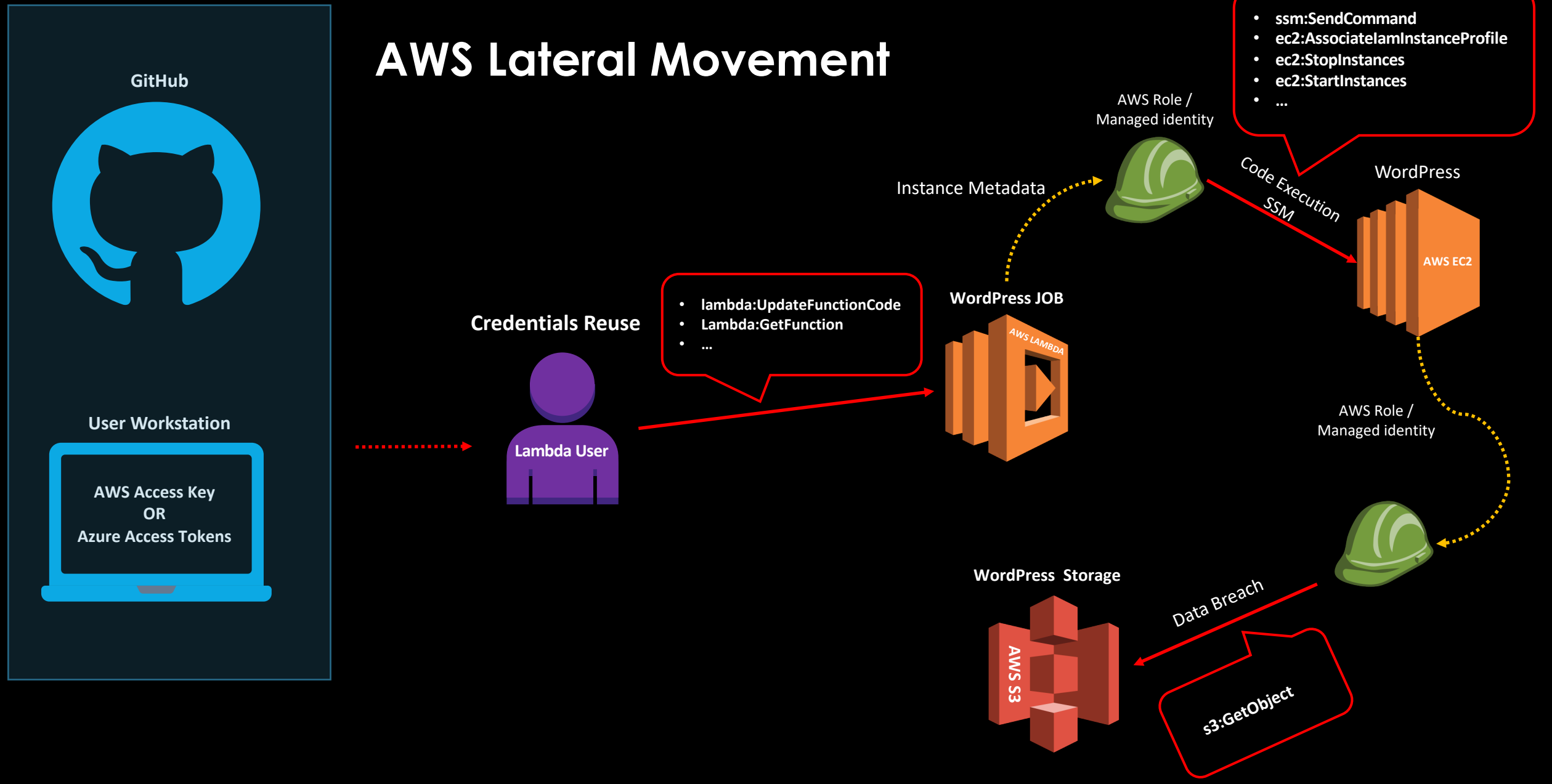
FUTURE WORK

THE PROBLEM WITH PUBLIC APIs

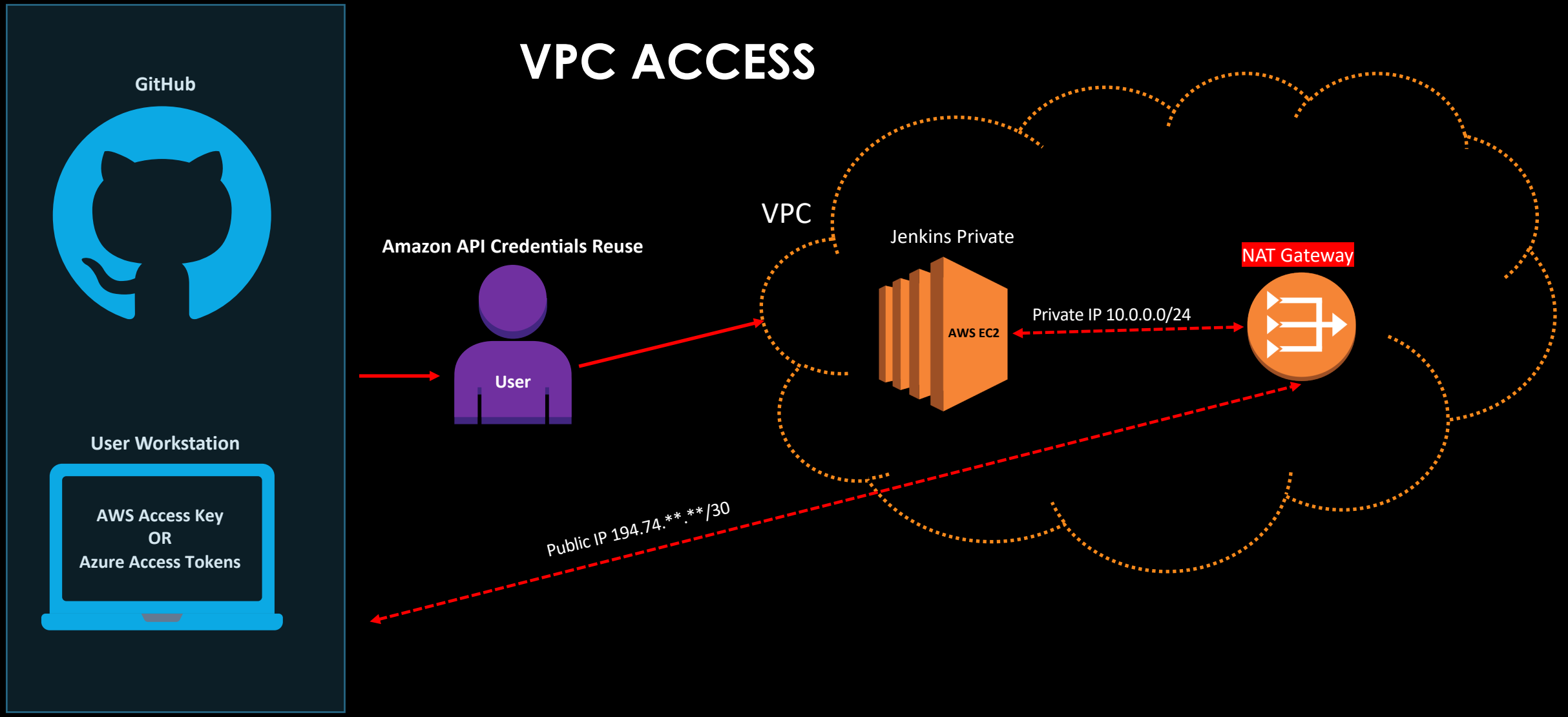
IDENTITY AND ACCESS MANAGEMENT

- IAM identities (users, groups of users, or roles)
- Policies and Permissions
- AWS resources
- Long-Term Access Keys
- Temporary security credentials (STS TOKEN)

AWS Lateral Movement



VPC ACCESS


GitHub
User Workstation
AWS Access Key
OR
Azure Access Tokens
Amazon API Credentials Reuse
User
VPC
Jenkins Private
AWS EC2
Private IP 10.0.0.0/24
NAT Gateway
Public IP 194.74.**.**/30

GRAPHS TO THE RESCUE!

BASIC ENTITIES (GRAPH NODE)

- User
- Access Key
- Managed Identities/Roles
- Public IP
- Virtual machines (EC2)
- Lambdas
- …

RELATIONS (GRAPH EDGES)

- Access Key To User
- Role To Lambda Lambda::GetFunction Permission
- Role To Lambda Lambda::UpdateFunctionCode Permission
- Lambda To Role
- Role to EC2 ec2::AttachVolume
- Role to EC2 ec2::DetachVolume
- Role to EC2 ec2:StartInstances
- Role to EC2 ec2:StopInstances
- …

ATTACK & READ ACCESS RELATIONS

- Access Key Usage - Access Key to User
- EC2 Instance Metadata Steal - EC2 to Role using the built-in machine role
- Lambda Instance Metadata Steal - Lambda to Role using the built-in role
- Lambda Modify Code - Connect Role to Lambda by modifying its code
- EC2 Storage Modify - Connect role to EC2 by changing it storage
- EC2 SSM Run Command - Connect role to EC2 by using the SSM Agent
- …

LIVE DEMO

FUTURE WORK

- Large Scale – Using Spark, Flink, etc
- Cloud Trail Support
- Simulation API
- Ease of Use

https://github.com/smulikHakipod/CloudSimulation

QUESTIONS?