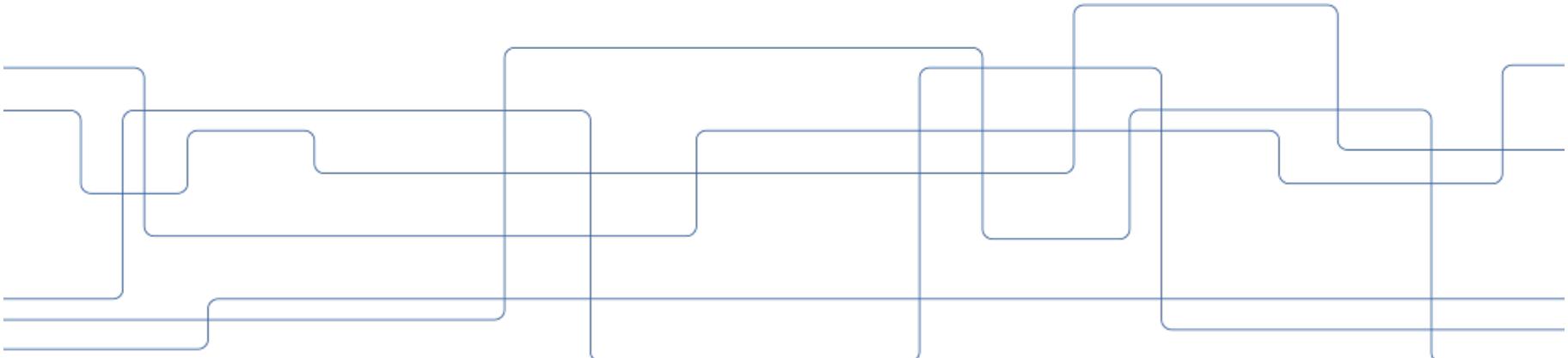




# CYBER SECURITY ASSESSMENT WITH ATTACK SIMULATIONS

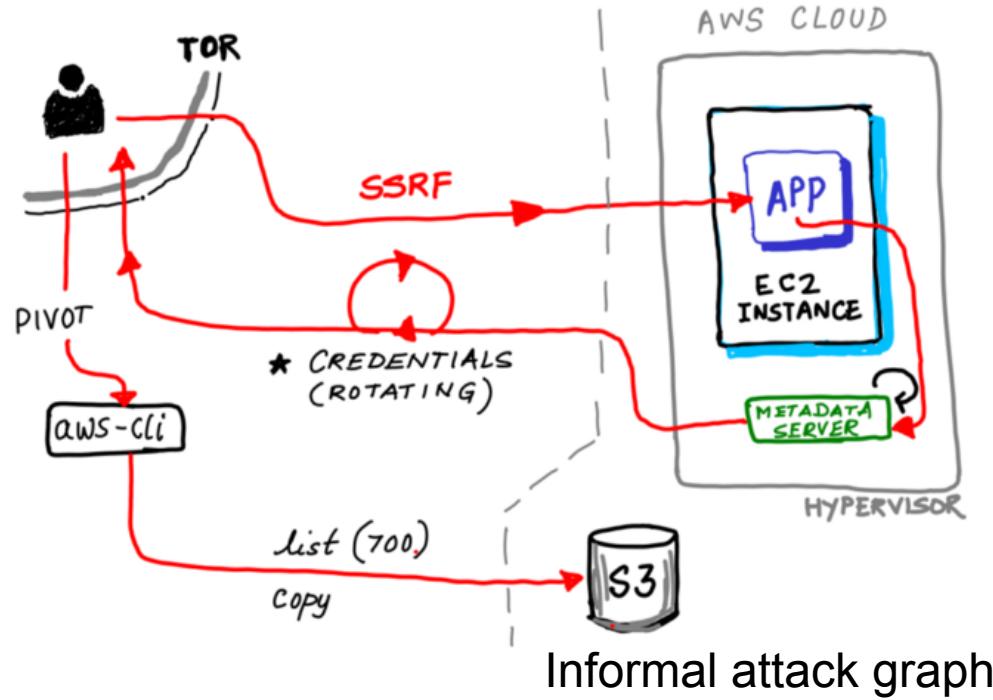
Pontus Johnson

Professor





# Capital One Breach in Amazon AWS



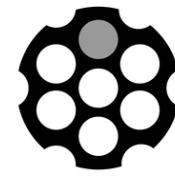
<https://blog.shiftleft.io/capital-one-breach-crime-board-case-of-speculative-sleuthing-e18fa937fa21>



# Risky Business Podcast on July 31, 2019



Adam Boileau & Patrick Gray



**RISKY.BIZ**  
It's a jungle out there

<https://risky.biz/RB550/>



# Risky Business Podcast on July 31, 2019



Adam Boileau & Patrick Gray

"Capital One are known for being really smart when it comes to this stuff, so when you see them getting owned by an attacker who falls into the category of Internet jerk, it does give you a moment."

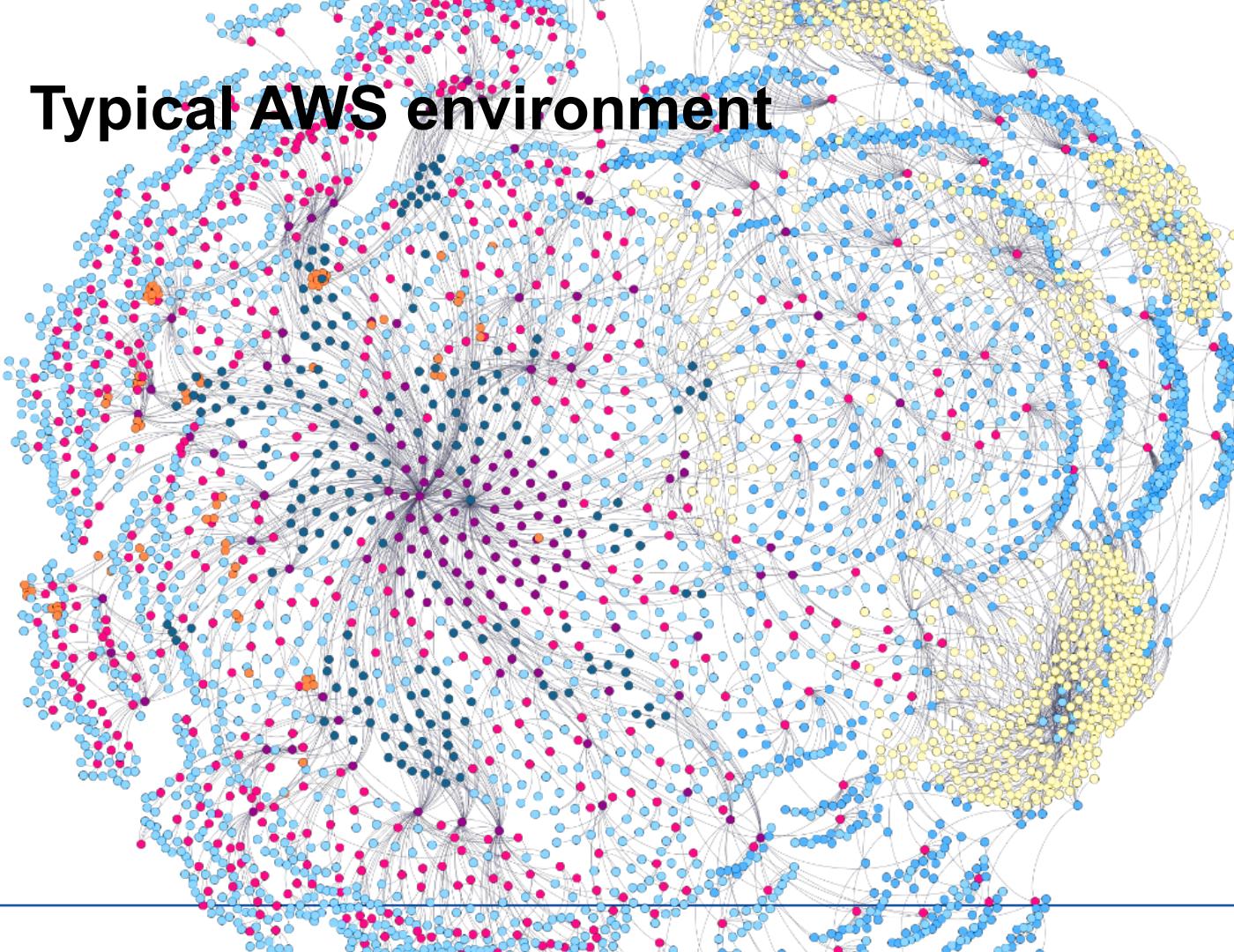
"Yes, part of the problem is that the Amazon product setup really is super complicated. You can build all sorts of amazing things at really big scale but doing it right consistently is really, really hard."

"A company that has some of the best people in the business for doing this stuff still got popped via their Amazon stuff because it is so complicated."



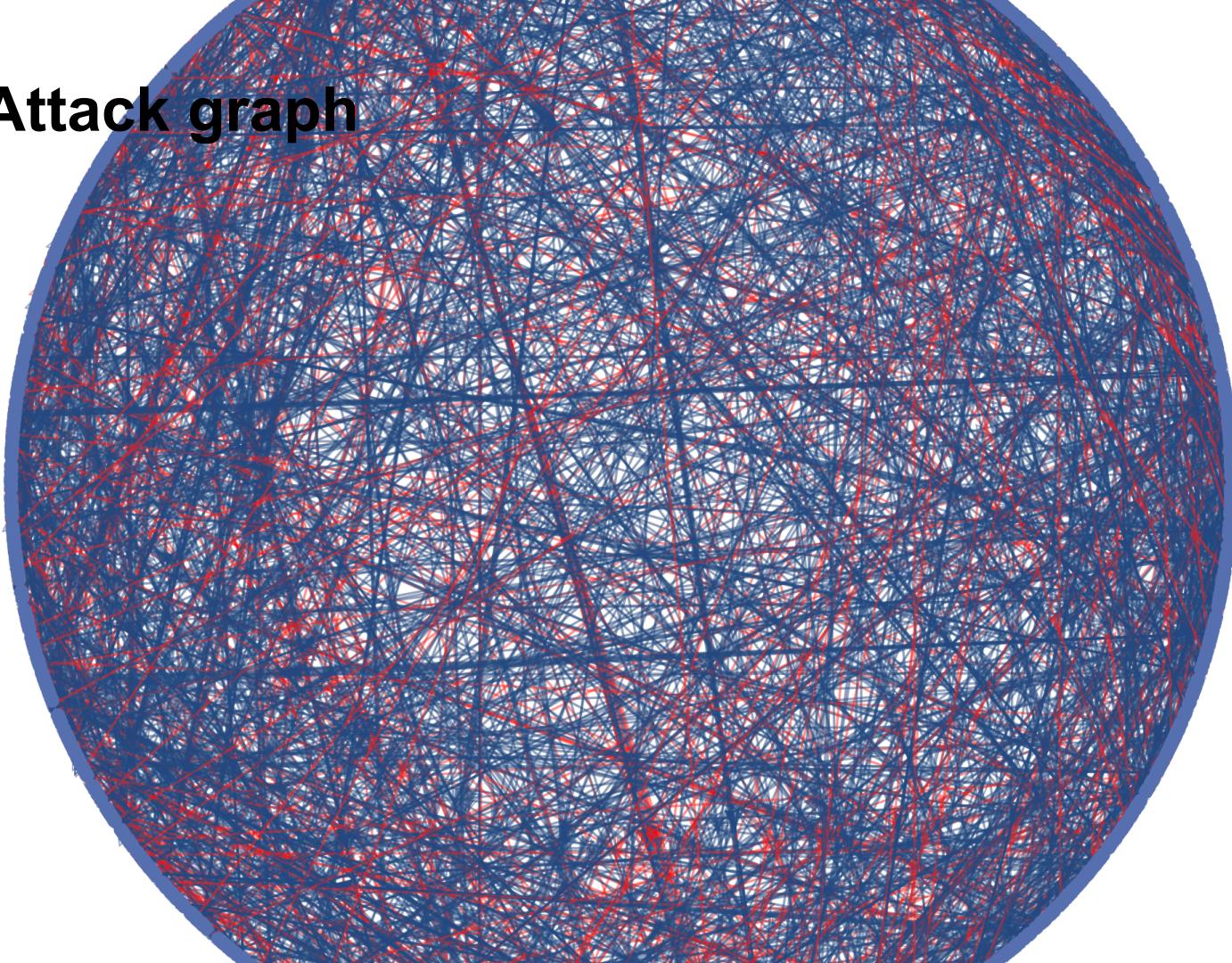


# Typical AWS environment





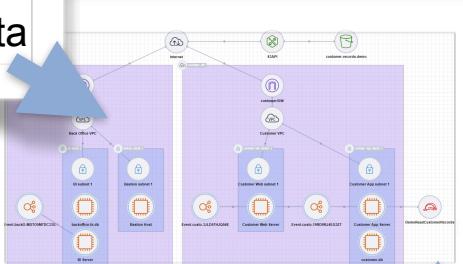
# Attack graph



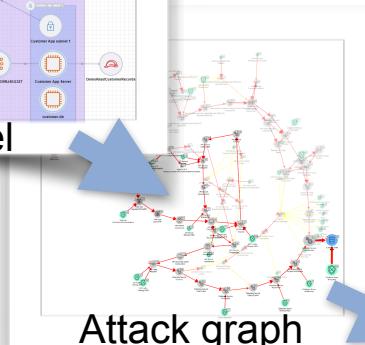


# Simulating cyber attacks

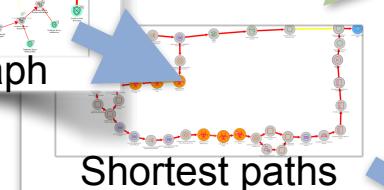
# AWS config data & vuln scan



AWS model



# Attack graph



# Shortest paths

## Simulation results

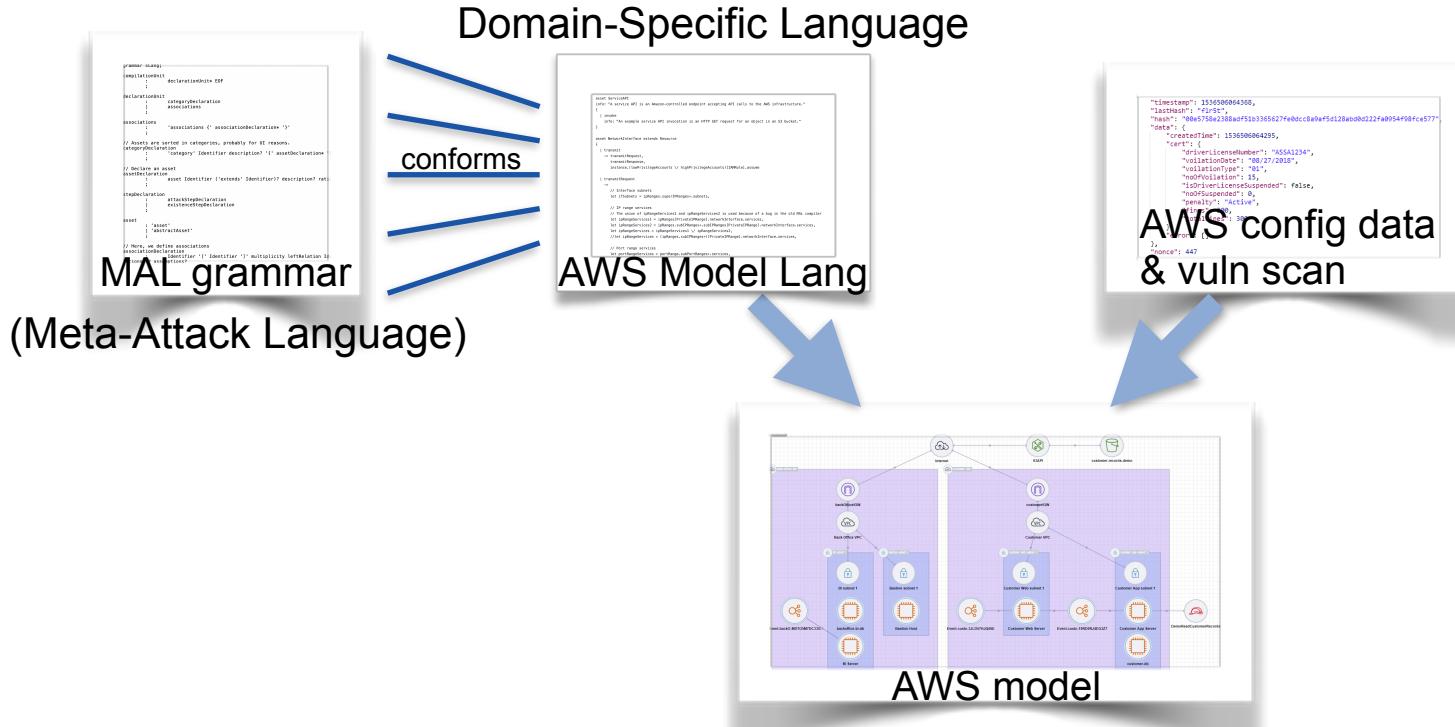
# The shortest paths an attacker can use to compromise assets of value

The easiest way for an attacker to reach the most valuable assets

# Mitigations



# Model generation



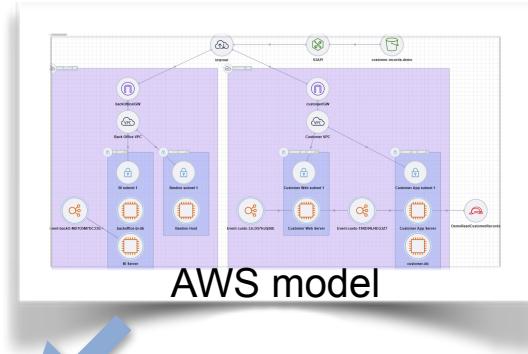
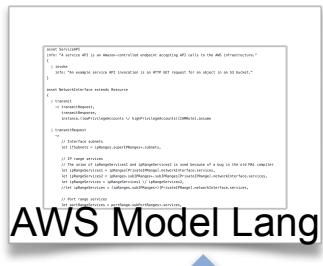


# AWS Domain-Specific Language (DSL) in MAL

```
[...]
asset EC2Instance extends Instance
{
}
[...]
asset S3Bucket extends Resource
{
}
[...]
associations {
S3Bucket [s3Bucket] 1 <-- Storage --> * [s3Objects] S3Object
[...]
```

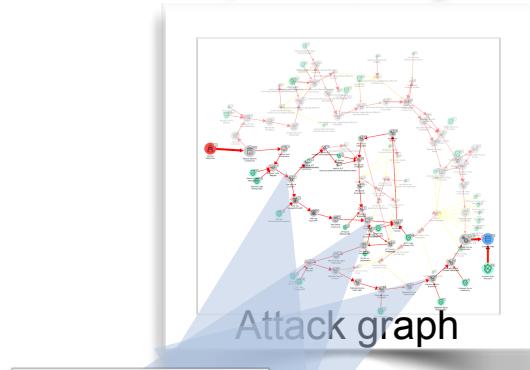


# Attack graph generation



AWS Model Lang

AWS model



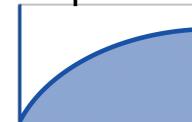
Local time to  
compromise

# AWS Domain-Specific Language (DSL) in MAL

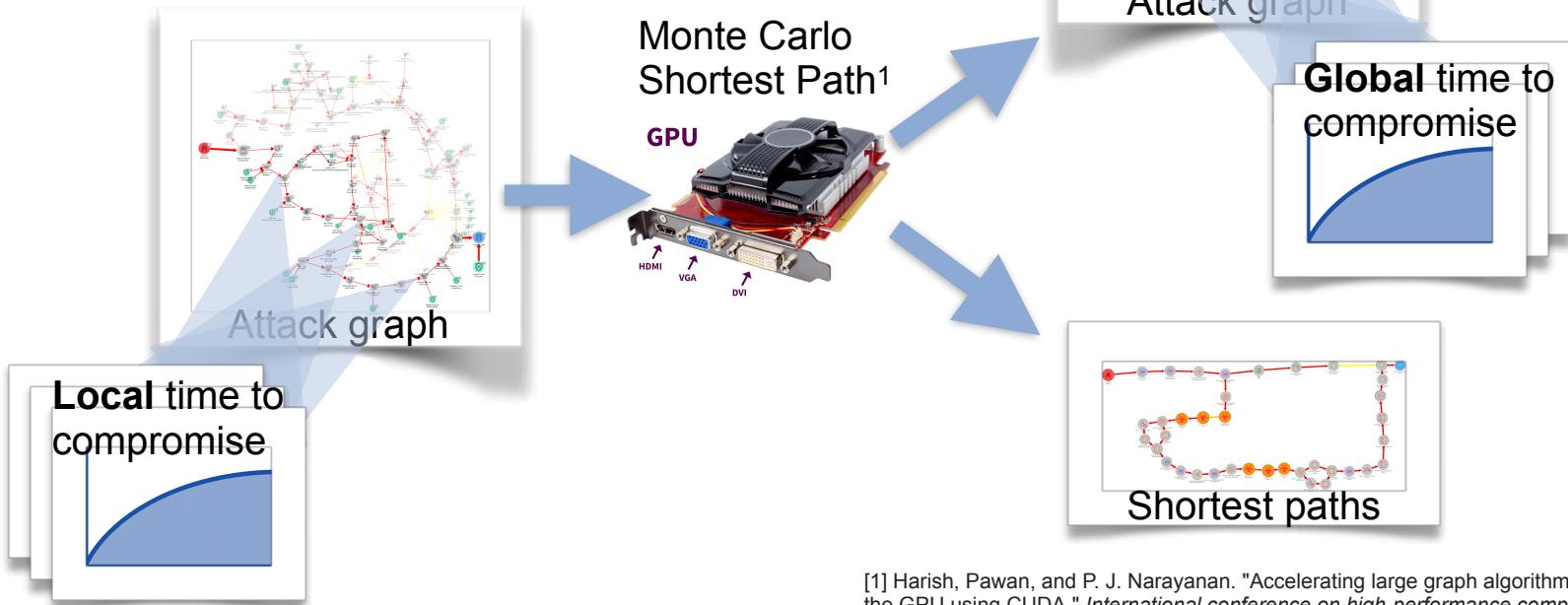
```
asset IAMIdentity extends Identity
{
    | assume
        -> policies.satisfy,
            statements.satisfy,
    [...]

abstractAsset HighComplexityVulnerability extends Vulnerability
{
    & abuse [ExponentialDistribution(x_hcv)]
        -> exploits.impact
}
[...]
```

Local time to  
compromise



# Attack graph computation



[1] Harish, Pawan, and P. J. Narayanan. "Accelerating large graph algorithms on the GPU using CUDA." *International conference on high-performance computing*. Springer, Berlin, Heidelberg, 2007.

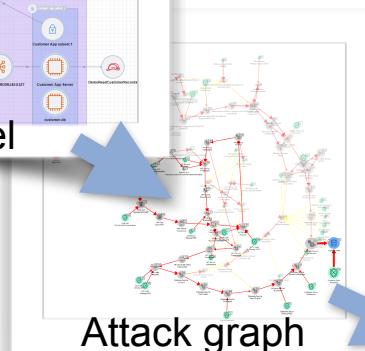


# Future works

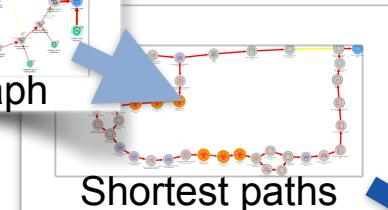
# AWS config data & vuln scan



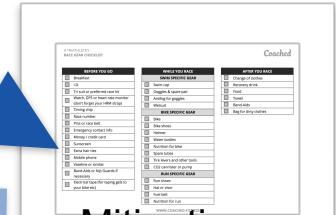
## AWS model



# Attack graph



# Shortest paths



# Mitigations



Home    About    Learn more    Who uses MAL?

Get Started



Meta Attack Language

*The open source platform for creation of cyber threat modeling systems*

Get Started →

<https://mal-lang.org>