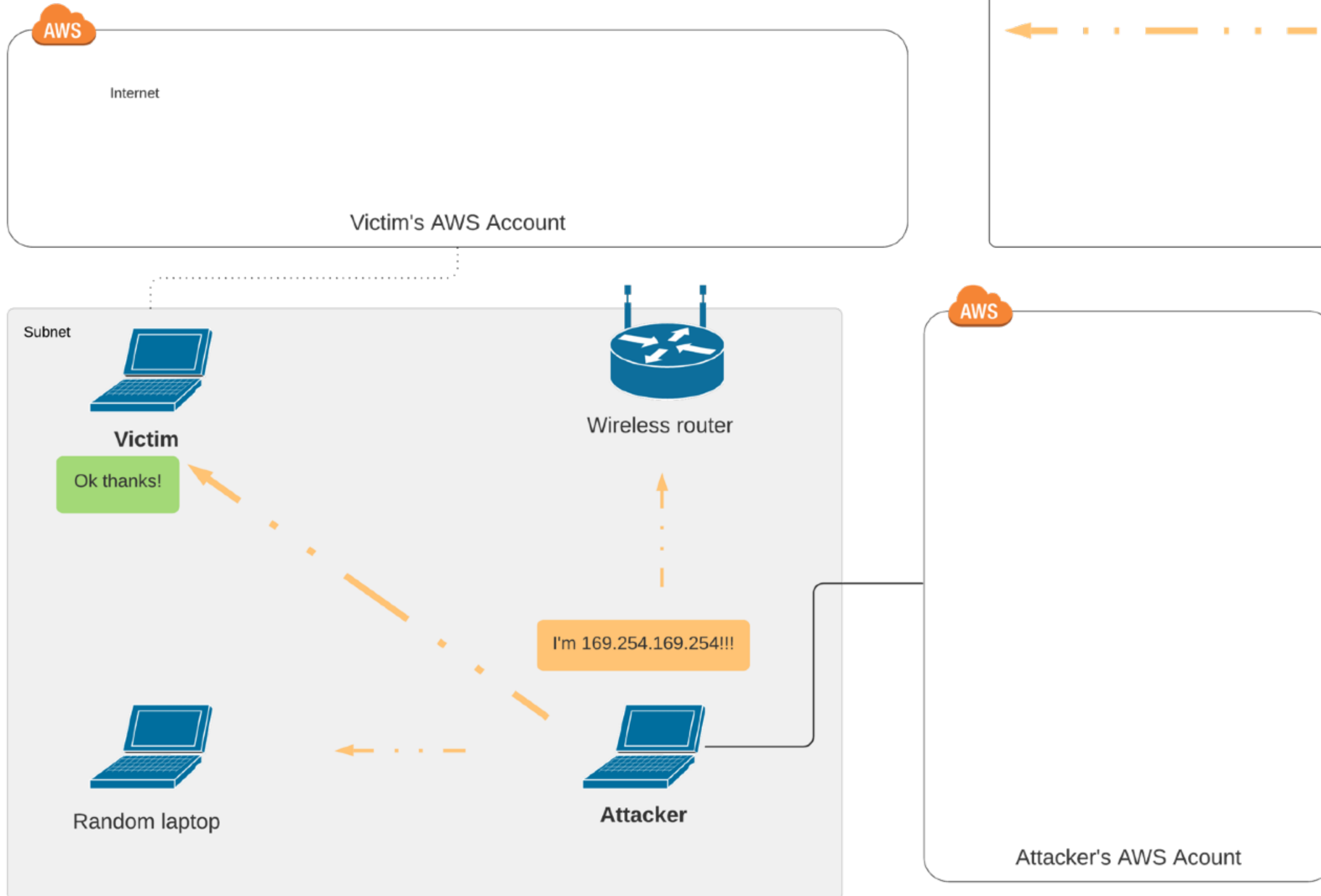


## IMDS Request Hijacking

Ryan Gerstenkorn | November 30, 2020



### Notes

1. Attacker responds to the ARP request. Claiming they own the IP, so traffic meant for it should be directed directly to them.

## IMDS Request Hijacking

Ryan Gerstenkorn | November 30, 2020

Legend

HTTP Request



HTTP Response



AWS

Internet

Victim's AWS Account

AWS

Attacker's AWS Account

Subnet



Victim

Can I have keys pls?



Sure, Here you go!



Attacker

### Notes

1. The victim thinks the attacker is the EC2 metadata server and issues an HTTP request to get credentials.