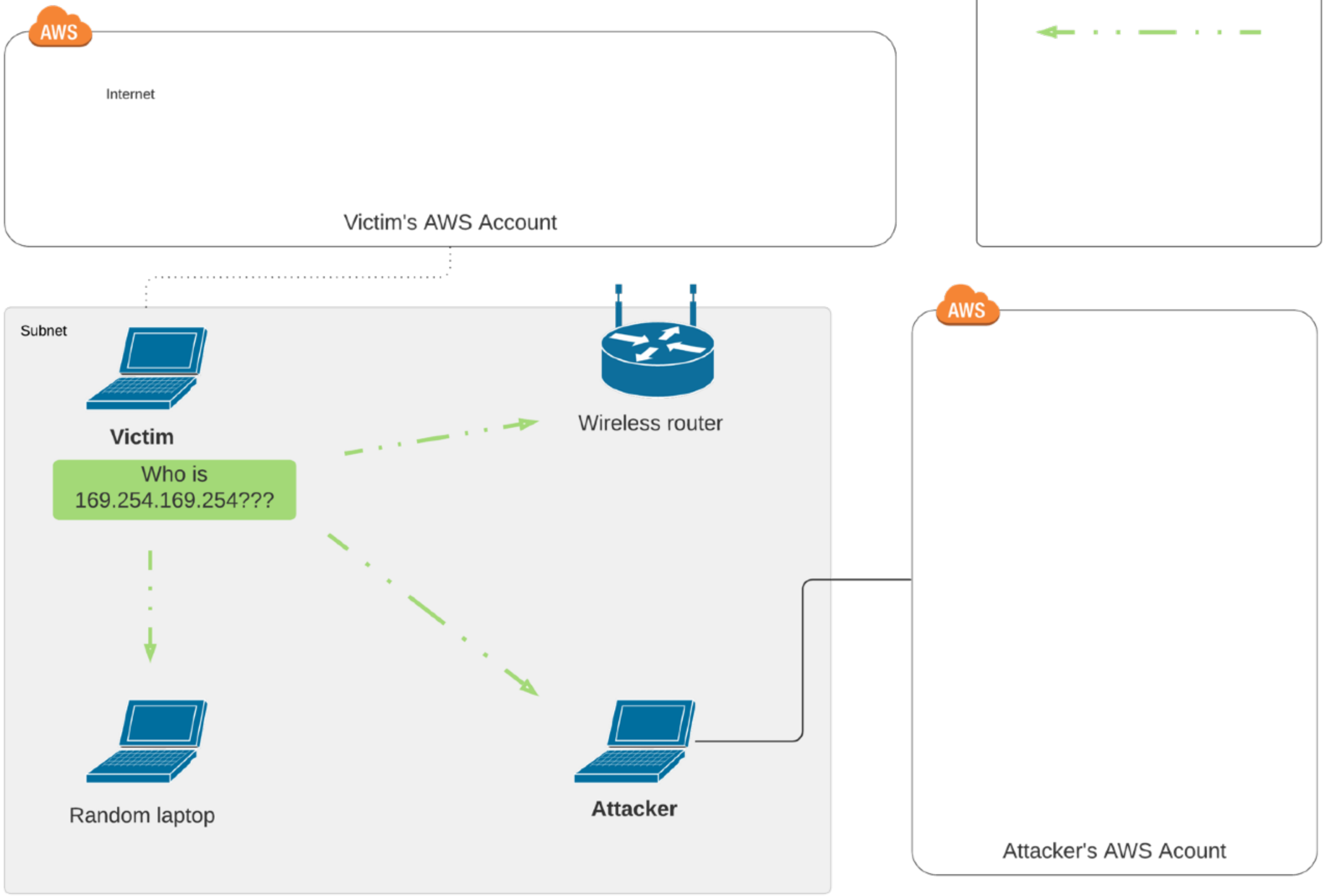
IMDS Request Hijacking

Ryan Gerstenkorn | November 30, 2020

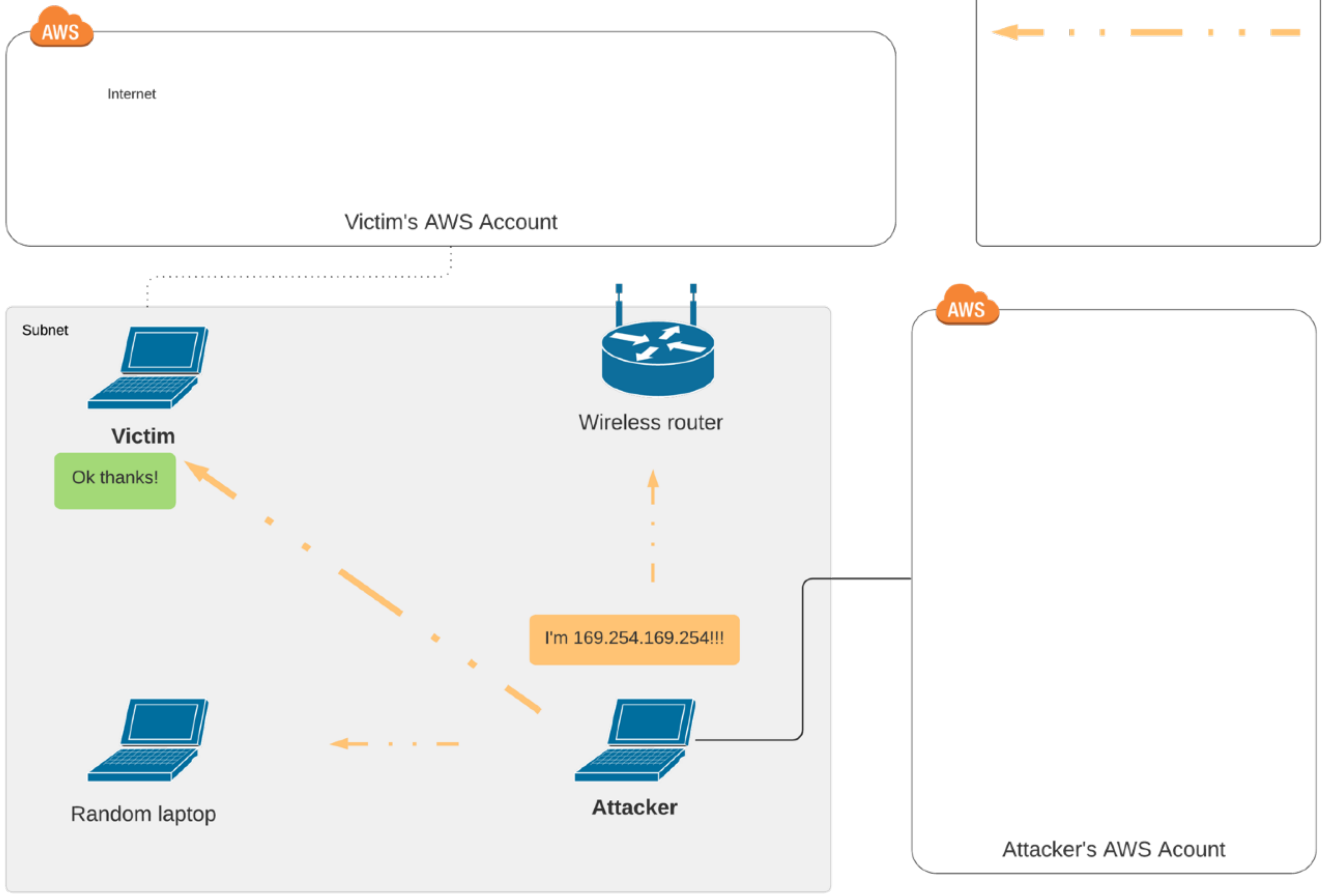


Notes

1. *ARP happens when the IP is in a range the host considers link-local.*
2. *Generally 169.254.0.0/16 is treated as link-local.*
3. *ARP is sent on the broadcast IP which means any host in the subnet can recieve and respond to it.*

IMDS Request Hijacking

Ryan Gerstenkorn | November 30, 2020



Legend

ARP Response

AWS

Internet

Victim's AWS Account

Subnet

Victim

Ok thanks!

Wireless router

I'm 169.254.169.254!!!

Random laptop

Attacker

AWS

Attacker's AWS Acount

Notes

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