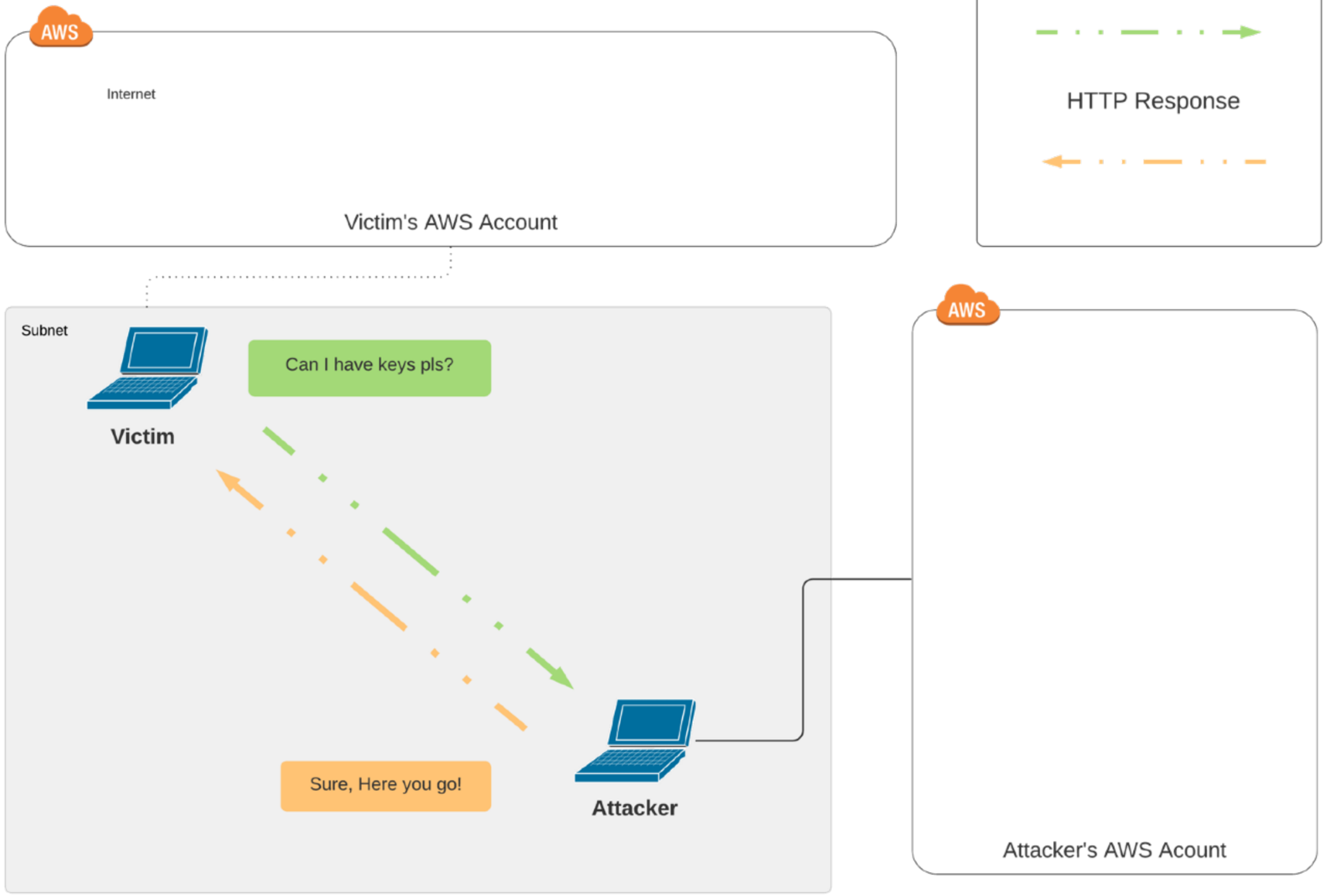
IMDS Request Hijacking

Ryan Gerstenkorn | November 30, 2020

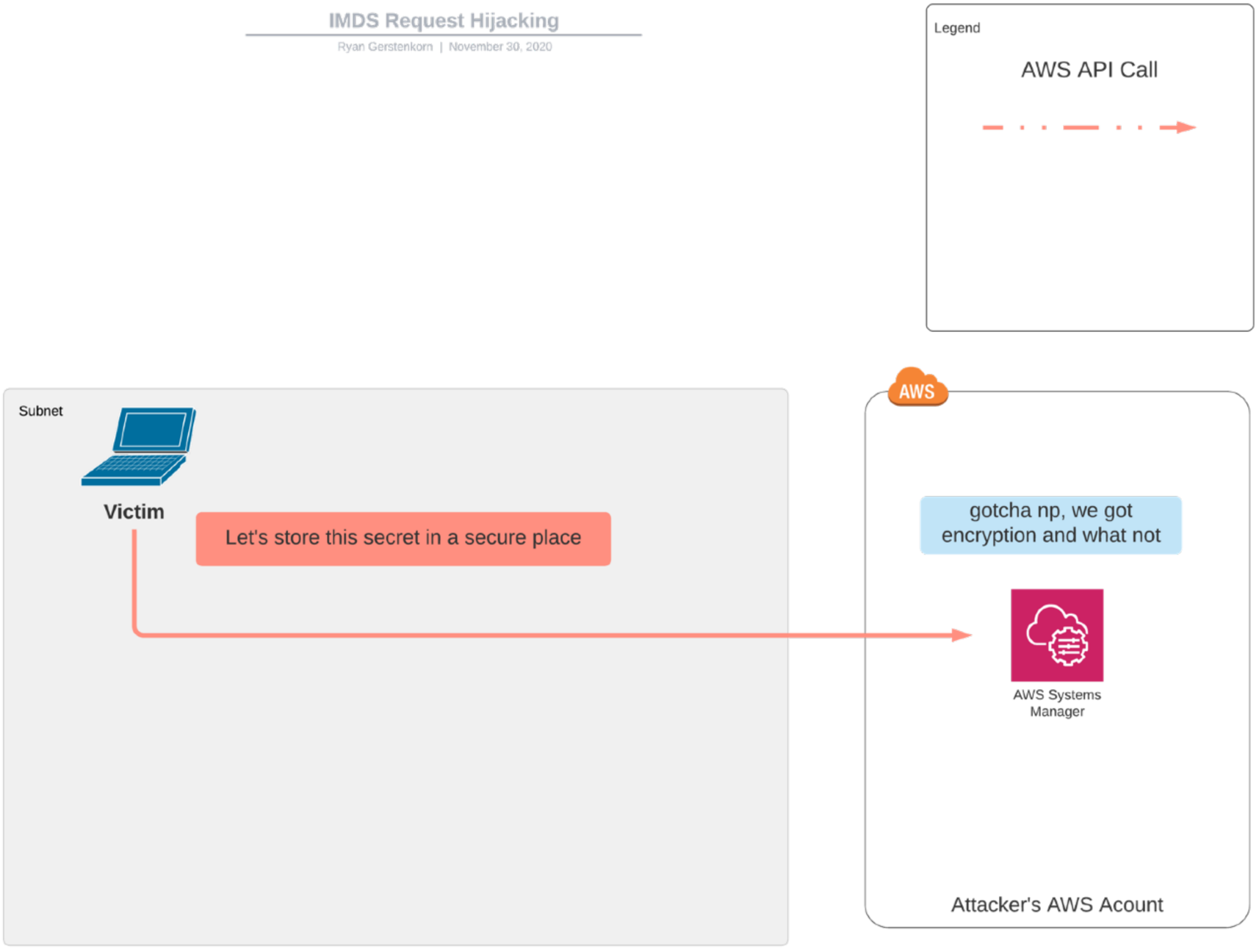


Notes

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

IMDS Request Hijacking

Ryan Gerstenkorn | November 30, 2020



Notes

1. *From this point on the victim will use the attacker's credential's when issuing API calls to AWS.*
2. ***Requests will fail with API calls that require an ARN, or certain expectations are made about the environment that don't match the attacker's account.***
3. *But if the attacker is lucky then the user may use an API call that is vulnable, such as SSM PutParameter. In which case the content/secret is uploaded to the attacker's account.*