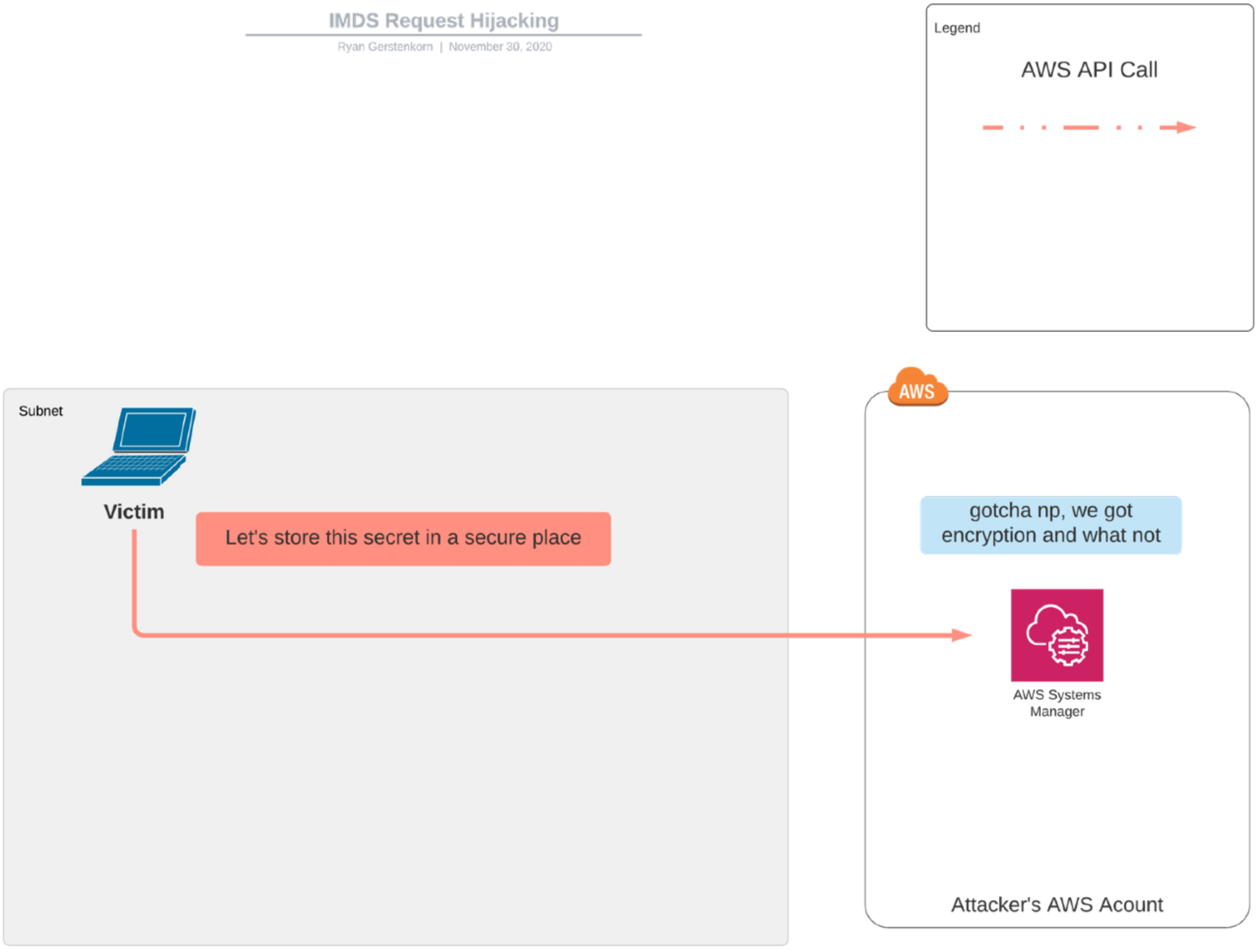
IMDS Request Hijacking

Ryan Gerstenkorn | November 30, 2020

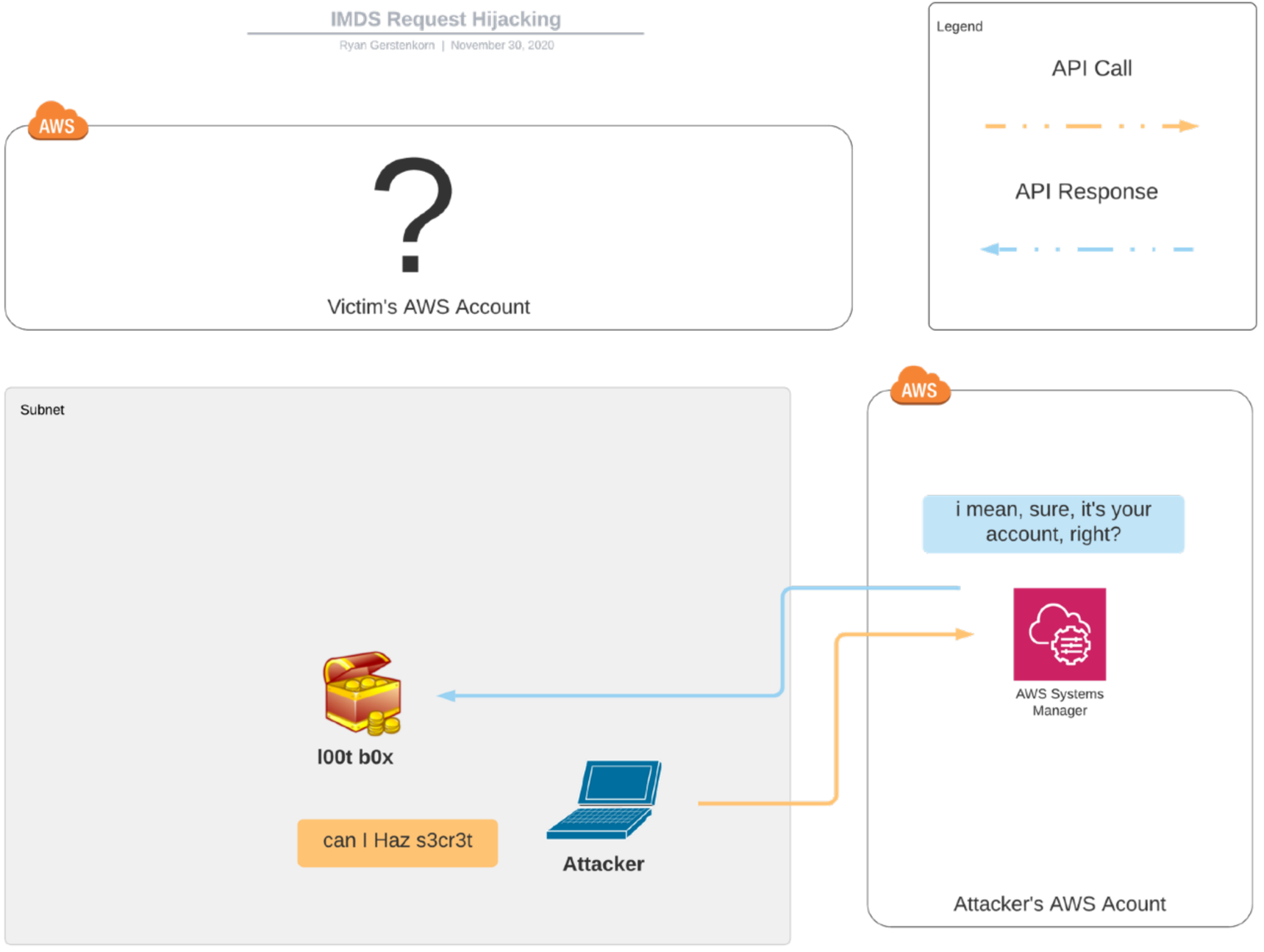


Notes

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.*

IMDS Request Hijacking

Ryan Gerstenkorn | November 30, 2020



Notes

1. ***Uploaded content can than be retrieved by the attacker, regardless of if it's (server side) encrypted or not.***
2. *In this specific example using a non-default KMS key however would have mitigated the issue. This is simply due to the API call requiring an ARN rather then a relative path.*
3. *However if the ARN is constructed through a get-caller-identity call, which is vulnable to this attack. It becomes possible (with a good bit of luck and skilll) for this attack to work again, despite a non-default KMS key being used.*