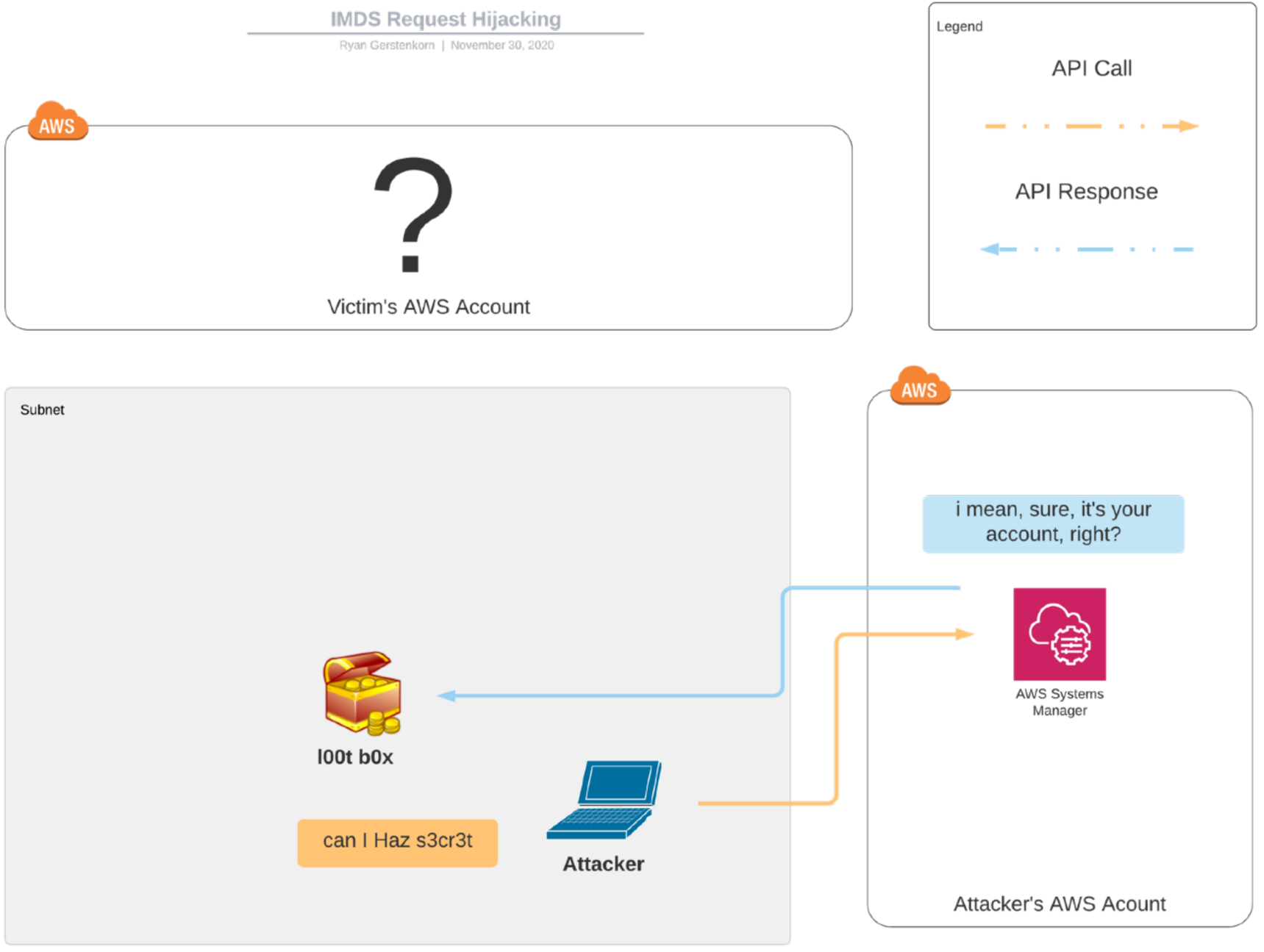
IMDS Request Hijacking

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.*

What else can we do with this?

- Collect Info about user's setups
  - SDK and OS Version
  - What API's are called (awscli v2.0.36 and newer)
- Map out resources via CloudTrail logs

```
PUT /latest/api/token HTTP/1.1
Host: 169.254.169.254
Accept-Encoding: identity
x-aws-ec2-metadata-token-ttl-seconds: 21600
User-Agent: aws-cli/2.0.36 Python/3.7.4 Darwin/19.6.0 exe/x86_64 command/s3.ls
Content-Length: 0
```